AFRL-RI-RS-TR-2016-210

VISITING SCHOLARS PROGRAM

STATE UNIVERSITY OF NEW YORK POLYTECHNIC INSTITUTE

SEPTEMBER 2016

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

AFRL-RI-RS-TR-2016-210 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/ S /
FRANKLIN E. HOKE, JR.
Work Unit Manager

/ S /
MARGOT R. ASHCROFT, Chief
Strategic Planning and Integration Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*
SEPTEMBER 2016

2. REPORT TYPE
FINAL TECHNICAL REPORT

3. DATES COVERED *(From - To)*
MAR 2013 – JAN 2016

4. TITLE AND SUBTITLE
VISITING SCHOLAR PROGRAM

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA8750-13-2-0115

5c. PROGRAM ELEMENT NUMBER
62788F

6. AUTHOR(S)
John Marsh

5d. PROJECT NUMBER
B2MS

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Research Foundation for SUNY
SUNY Polytechnic Institute
100 Seymour Road
Utica, NY 13502

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/RIBA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2016-210

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Research Foundation (RF) for SUNY Polytechnic Institute (SUNY Poly) has contributed significant research capability and capacity to the In-House program at AFRL through the placement of highly motivated and accomplished faculty members and graduate students pursuing advanced degrees in Engineering, Computer Science, Mathematics and other recognized technical disciplines critical to the advancement of Information technologies. SUNY Poly worked closely with AFRL to help build, foster, and nurture in-house research teams. Under this effort SUNY Poly recruited, placed and supported administrative requirements for 42 faculty members and 17 undergraduate/graduate research assistants and coordinated an additional 54 faculty extension efforts. This report contains abstracts from annual final technical reports from fundamental research performed through a summer research program and other associated grants.

15. SUBJECT TERMS
SUNY Poly, STEM, Artificial Intelligence, Command and Control

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** **FRANKLIN E. HOKE, JR.**
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	70	**19b. TELEPHONE NUMBER (*Include area code*)** **NA**

TABLE OF CONTENTS

1. INTRODUCTION

The State University of New York Polytechnic Institute (SUNY Poly; formerly Institute of Technology), has facilitated the management of the Air Force Research Laboratory Information Directorate Visiting Faculty Research Program. SUNY Poly places highly qualified and motivated faculty members and students (B.S., M.S. and Ph.D.) in science, technology, engineering and mathematics (STEM) disciplines as well as other recognized technical and newly emerged interdisciplinary areas to provide an intellectually stimulating research environment for selected participants a rewarding experience.

Included in this report are short abstracts of the research conducted in collaboration with AFRL/RI Information Institute scientists and engineers.

FACULTY & RESEARCH AREAS

1.1. 2013 Summer Professors

Howard A. Blair – Self-Correcting Quantum Dynamical Systems; Department of Electrical Engineering and Computer Science, Syracuse University

A self-correcting dynamical system, quantum or classical, it is a system with an evolving state in which errors due to stochastic variation in computed values are damped out during execution by means intrinsic to the rules for state evolution and not specifically by auxiliary error correction. Such dynamical systems are said to be robust against noise in this specific sense. One approach to obtaining such systems is via evolutionary programming techniques in which a suite of properties of the trajectories of the system are extracted during executions and used to obtain a preference ordering among the system's trajectories. From such a preference ordering the rules of the evolution of the system's state, its trajectory, can be altered, usually by adjusting control parameters, to produce a more preferred to the trajectory. The preference ordering can be obtained from either quantitative information or structural information or both.

Executing programs are dynamical systems. Although the state space of an executing program is always discrete, executing programs are often intended to model continuous systems. In such circumstances the program's execution trajectories in its state space can be seen as discretizations of continuous trajectories in an associated phase space. Such a discretization can, in turn, be seen as injecting noise into the production an ideal continuous trajectory and the program with its discrete state space is thus a noisy approximation to a continuous dynamical system. If the continuous system is contractive in envelopes around its desired trajectories and the discretized system produces states within these envelopes, the discretized system will closely shadow the desired trajectories within the ideal continuous system.

It is often desirable to have at least some aspects of a system's trajectory stable against moderate noise. To achieve this one can identify and exploit strange attractors in the system's dynamics. Any stochastic variation in the salient aspects of the system's trajectory are implosively damped out as the state evolves. It is difficult to find strange attractors, if any, in a system's dynamics, and more difficult to exploit them, but this problem is exactly where genetic algorithms and evolutionary programming techniques shine.

Jian-Feng Cai – One-Bit Compressed Sensing of Images by Total Variation Minimization; Department of Mathematics, The University of Iowa

In this report, we study one-bit compressed sensing of images that are modeled by bivariate functions with sparse gradients. We establish the proof for the performance of total variation (TV) minimization in recovering images with sparse gradient support from the signs of small amount of Gaussian measurements. In particular, we showed that an $n \times n$ image with s nonzero gradients can be recovered from the signs of its $O(s \log_2(n) \log(n_2/s))$ random linear measurements. The result is an extension of the one-bit compressed sensing theory in *One-bit compressed sensing by linear programming*, Communications on Pure and Applied Mathematics, (2013).

Yiren Chen – A Framework of Heterogeneous Computing Systems with Compact Memristor-based Neuromorphic Computing Accelerators; Electrical and Computer Engineering Department, University of Pittsburgh

As technology scales, on-chip heterogenous architecture emerges as a promising solution to combat the power wall of microprocessors. In this work, we propose Harmonica, a framework of heterogeneous computing systems with memristor-based neuromorphic computing accelerators (NCAs). In Harmonica, NCA is designed to speedup the artificial neural network (ANN) executions in many high-performance applications by leveraging the extremely efficient mixed-signal computation capability of nanoscale memristor-based crossbar (MBC) arrays. The hierarchical MBC arrays of the NCA can be flexibly configured to different ANN topologies through the help of an analog Network-on-Chip (A-NoC). Our simulation results show that compared to the baseline general purpose processor, Harmonica can achieve on average 18.2% performance speedup and 20.1% energy reduction over the simulated nine representative applications. The computation accuracy degradation is constrained within an acceptable range.

Edwin E. Hach, III – Robust, Scalable Hong-Ou-Mandel Manifolds in Quantum Optical Ring Resonators – *And* – Finite Violations of a Bell Inequality by Entangled SU Coherent States; School of Physics and Astronomy, Rochester Institute of Technology

Quantum Information Processing, from cryptography to computation, based upon linear quantum optical circuit elements relies heavily on the ability offered by the Hong-Ou-Mandel (H-O-M) Effect to “route” photons from separate input modes into one of two common output modes. Specifically, the H-O-M Effect accomplishes the path entanglement of two photons at a time such that no coincidences are observed in the output modes of a system exhibiting the effect. In this paper, we prove in principle that a significant increase in the robustness of the H-O-M Effect can be accomplished in a scalable, readily manufactured nanophotonic system comprised of two waveguides coupled, on-chip, to a ring resonator. We show that by operating such a device properly, one can conditionally “bunch” coincident input photons in a way that is far more robust and controllable than possible with an ordinary 50/50 beam splitter.

Hai Li – General Realization of Neuromorphic Computing Systems Based on Stochastic Characteristics of Memristive Switches; Electrical and Computer Engineering Department, University of Pittsburgh

Memristor–the fourth basic circuit element, has shown great potential in neuromorphic circuit design for its unique synapse-like feature. However, a large gap still exists between the theoretical memristor characteristics and the experimental data obtained from real device measurements. For instance, though the continuous resistance state of memristor has been expected to facilitate neuromorphic circuit designs, obtaining and maintaining an arbitrary intermediate state cannot be well controlled in nowadays memristive system. In addition, the stochastic switching behaviors have been widely observed. To facilitate the investigation on memristor-based hardware implementation, we built a stochastic behavior model of TiO_2 memristive devices based on the real experimental results. By leveraging the stochastic behavior of memristors, a macro cell design composed of multiple parallel connecting memristors is proposed, providing a feasible solution in memristor-based hardware implementation of neural networks.

Chen Liu – Adaptive Virtual Machine Management in the Cloud - A Performance Counter Driven Approach; Department of Electrical and Computer Engineering, Clarkson University

The success of cloud computing technologies heavily depends on both the underlying hardware and system software support for virtualization. In this study, we propose to elevate the capability of the hypervisor to monitor and manage the co-running VMs by capturing their dynamic behavior at runtime and adaptively schedule and migrate VMs across cores to minimize the contention on system resources hence maximize the system throughput. Implemented at the hypervisor level, our proposed scheme does not require any changes or adjustments made to the VMs themselves or the applications running inside them, nor to the host OS. It also does not require any changes to existing hardware structures. These facts reduces the complexity of our approach at the same time improves portability. Through initial implementation, our experimental results show the presented approach is of great potential to improve the overall system throughput in the cloud environment.

Jing Peng – Investigation into Observed Performance Difference Between ShareBoost and rShareBoost; Computer Science Department, Montclair State University

We have developed an algorithm, called ShareBoost, for combining mulitiple classifiers from multiple information sources. The algorithm builds base classifiers independently from each data type (view) that provides a partial view about an object of interest. Different from AdaBoost, where each view has its own re-sampling weight, ShareBoost uses a single re-sampling distribution for all views at each boosting round. This distribution is determined by the view whose training error is minimal. We have also developed a randomized version of the algorithm, where a winning view is chosen probabilistically. Both algorithms have shown promise in a number of applications. While rShareBoost is more efficient computationally than ShareBoost, it is expected that rShareBoost should exhibit slow convergence given the same number of base classifiers. However, experimental results have shown that the opposite is true. This report provides the insight into this surprising observation.

Madjid Tavana – A Deterministic Risk Analysis and Measurement Model for Assessing Availability and Integrity in Command and Control Systems; Business Systems and Analytics Department, La Salle University

Military Command and Control (C2) systems are increasingly challenged by a host of modern problems, namely, internal vulnerabilities and external threats. Several approaches have been suggested in the literature to measure availability and integrity in C2 systems. Despite the importance of developing and maintaining self-protecting and self-healing processes, the simultaneous consideration of availability and integrity has received little attention in the literature. We propose a deterministic Quantitative Risk Analysis and Measurement (Q-RAM) framework for C2 systems which is focused on the failure risk induced by internal vulnerabilities and external threats present in the C2 systems. The proposed system allows risk managers to get a comprehensive snapshot of the system availability and integrity, assess the failure risks with the assistance of a multi-factor risk metric, and manage those risks by searching for the best combination of countermeasures, allowing the user to determine the preferred tradeoff between the system's availability and integrity costs.

Dmitry Uskov – Photonic Quantum Information Processing; Division of Mathematics and Science, Brescia University

The focus of this research was on developing novel theoretical and experimental schemes and algorithms exploiting quantum properties of photonic Hilbert space. Suggested research proposal has its roots in our previous work on numerical optimization of linear optical quantum gates, cluster state generation, and quantum metrology. Numerical and analytical toolbox developed by us for solving optimization problems for linear optical computation was applied for a completely new set of tasks: testing the limits of efficiency of photonic quantum information processing by redesigning existing schemes and algorithms in order to obtain their optimal photonic implementation.

Kai Zeng – Physical Layer Challenge-Response Authentication in Wireless Networks with Relay; Department of Computer and Information, Science University of Michigan

Exploiting physical layer characteristics to enhance or complement authentication strength in wireless networks has been attracting more research attention recently. Existing physical layer authentication mechanisms mainly tackle single-hop communications. In this paper, we propose two physical layer challenge-response authentication mechanisms for wireless networks with relay. One mechanism, named PHY-CRAMR, is an extension of the existing PHY-CRAM protocol. It fully utilizes the randomness, reciprocity, and location decorrelation features of the wireless fading channel to hide/encrypt the challenge response messages at the physical layer, and is immune to outside attacks with a trusted relay. The other novel mechanism, named PHY-AUR (PHYsical layer Authentication with Untrusted Relay), exploits randomness, coherence, and location decorrelation properties of wireless fading channel to securely convey the product of the channel state information on consecutive links and use the fading channel to encrypt challenge and response messages. PHY-AUR is immune to both outside and inside attacks with an untrusted relay. Both PHY-CRAMR and PHY-AUR adopt the orthogonal frequency division multiplexing (OFDM) technique to modulate the authentication key and challenge-response messages on subcarriers. Physical layer pilots and preambles are eliminated to prevent an attacker from gaining knowledge about the channel state information, and as a result prevent the authentication key from being revealed to untrusted attackers. We analyze the security strength of both mechanisms and conduct extensive simulations to evaluate them. It shows that both PHY-CRAMR and PHY- AUR can achieve both a high successful authentication rate and low false acceptance rate, and the performance improves as the signal to noise ratio (SNR) increases.

1.2. 2014 Summer Professors

Rida Bazzi – Towards Moving Target Defense With Guarantees; School of Computing Informatics and Decision Systems Engineering, Arizona State University

Existing moving target defense schemes are uncomfortably rooted in existing attacks which makes their effectiveness in protecting against future attacks unquantifiable. The goal of the work is to explore the possibility of developing a moving target defense with guaranteed security properties with minimum assumptions about the attacker capabilities. The document has two parts addressing damage potential and moving target defense. The frst part addresses shortcoming of existing damage potential and attack surface measures. In particular, current treatment of damage potential does not directly reflect the actual damage that can result from compromised resources. We propose a new measure of damage potential that better captures the actual damage that can occur due to system vulnerabilities. We argue that having an accurate measure of damage potential is essential for developing moving target defense with guarantees (MTDG). We propose elements of what an MTDG can look like.

Upendranatha Chakravarthy – Evaluation of Stream and Complex Event Processing (SEP) Framework for Video Analysis and Fusion; Computer Science and Engineering Department, The University of Texas at Arlington

Complex event Processing (CEP) has come a long way (since the Eighties) from adding simple monitoring capabilities – in the form of triggers – to Database Management Systems (termed active DBMSs) to process continuous, varying input rate data and event streams from sensors and other applications (e.g., UAVs). The requirements as well as the capabilities needed for newer applications have changed drastically from its beginnings. Many event specification languages, optimization techniques for processing live as well as collected data (termed event logs in the event processing community and forensics in the video processing community, respectively) have been developed. Distributed applications have additional issues on computation distribution, fault-tolerance, and recovery aspects of CEP.

Stream processing (SP) became relevant mainly due to inexpensive and hence ubiquitous deployment of sensors in many applications (e.g., environmental monitoring, battle field monitoring). Other continuous data generators (web clicks, traffic data, network packets, mobile devices) have also prompted processing and analysis of these streams for applications such as traffic congestion/accidents, network intrusion detection, and personalized marketing.

Although SP and CEP are used in many diverse application domains, surprisingly, these technologies have not been exploited for video analysis and fusion to the best of our knowledge. Situation awareness requires, collecting, aggregating, and analyzing disparate data types (e.g., video, sensor, audio, call reports) in order to make informed decisions. If it is a realtime or near real-time decision making (surveillance as compared to forensics where archived data is analyzed), additional real-time processing and interactive requirements become critical. Video analysis and extraction of relevant content characteristics are also processing-intensive and requires computations that are very different from those used on categorical and numeric data. Moreover, modeling of complex situations using events and aggregation of components of video analysis is not straightforward. As a result, video analysis and fusion has focused on customized solutions for specific problems (e.g., object identification, object classification, overlaps of objects, tracking object movements.) A large number of techniques (both pattern recognition-based and machine learning-based) for processing video frames to characterize objects have been developed to deal with camera angles, lighting effects, color differences, as well as object identification and re-identification. Feature extraction, segmentation, and separation of background from foreground use numerous algorithms and machine learning techniques to deal with specific application domains. Also, the input quality and characteristics vary quite significantly among video streams (based on frame rate, pixel density, and appliances used, etc.) which necessitates the use of specific algorithms and approaches. Of course, the image processing technology is continuously improving as also the collection technology.

The focus of this work is to evaluate the applicability of stream and complex event processing techniques to video analysis and fusion applications with the intent of leading to alternative, high-level specification of situations, their mapping to well-defined lower level operators and their computation, optimization, and subsequently reasoning about quality of service (QoS), capacity modeling, as well as parallelization. The higher-level specification will also help in translating or mapping general situations (e.g., track an object where the object can be specified as a parameter) into their corresponding computations. In this report, we first provide an extensive survey of the traditional SP and CEP literature (as it is targeted to readers from image analysis, video processing, and fusion background who may not be familiar with the work on stream and complex event processing) to understand the current state-of-the-art including a stream and event processing (SEP) architecture developed by the author. We then survey and analyze the problem of video analysis to understand the problem clearly, its nuances, differences between the two in terms of computation, real-time needs, complexity of situations to be represented, and other requirements. The larger problem we are interested in is fusion which involves multi-modal inputs (from sensor data to reports to images, and video) to understand the correlation (and hopefully causation) between various inputs to gain situation awareness (SAW). Video analysis seems to be a good starting point for this work.

We then evaluate the relevance of the various data representations and operators proposed for traditional stream and sequence processing. We identify and propose a representation that may be appropriate for capturing the contents of video frames for further processing. We also present a set of operators (or application of available operators) that are appropriate for video analysis using a number of applications and contexts to drive the requirement. We define operators and their semantics in the context of video analysis. The computational aspects of these operators are also considered to understand potential optimizations that can be developed later. Finally, we provide examples of the usage of the operators for expressing specific situations.

Typically, images and video frames are pre-processed and relevant information extracted and represented in different ways depending upon the needs of the subsequent processing. As there are a large number of techniques available for pre-processing images for various needs, the ability to include pre-processing of images in different ways into our framework is extremely important. We propose an approach to express and compute the desired representation using sequence processing operators.

Once the operators are identified and defined along with their semantics, the next step (beyond this summer program and its extension) would be to incorporate them into a stream processing architecture to develop a prototype for testing and experimentation. The traditional SP and CEP system MavEStream developed by the author can be used for this purpose by replacing its operators (such as relational Join) with new operators. Also, the operators need to work with the chosen data representation which is likely to be different from the current representation which is a relational table with numerical and categorical data. This approach to develop a prototype will be faster as several features of stream processing, such as the notion of a window, scheduling, and other features can be re-used. This architecture is also presented in this report. However, this architecture needs to be revised to include different algorithms (e.g., comparing feature vectors) and extended to include the human in the loop and provide interfaces which makes it easy to understand what is going on. This is an extremely important aspect of video-based situation monitoring which is typically lacking in traditional stream and event processing.

Once a prototype is available, it can be evaluated for various application scenarios – for expressiveness, latency measurements, and its ability to provide feedback for the human in the loop. This will further lead to optimization and improvement for new situations.

Another aspect of video and image analysis (as well as fusion) that seems to be important is forensics. This is the ability to piece together a story line or to create a representation over which queries can be posed and inferences be drawn to understand different“what-if” situations. The example given for this need is the way in which“Boston bombing” incident was analyzed by humans using large amounts of images and video from various, unrelated sources to construct a plausible story line. Similar work for understanding patterns in a city using traffic and other videos are also underway.

Wenliang (Kevin) Du – Code Injection Attacks on HTML5-based Mobile Apps; Department of Electrical Engineering & Computer Science, Syracuse University

HTML5-based mobile apps are becoming more and more popular due to their portability advantage. Adobe's PhoneGap is a mobile development framework which enables software programmers to build applications for mobile devices using JavaScript, HTML5, and CSS3. In this presentation, we report on risks and vulnerabilities of HTML5-based mobile apps, and also introduce our detection and patching technologies to protect mobile apps against attacks. The web technologies used by HTML5-based apps allow data and code to be intermixed, making code injection attacks possible. First, we discuss our work on thwarting such attacks in HTML5-based mobile apps. We concentrated on a new form of code injection attack, which inherits the fundamental cause of Cross-Site Scripting attack (XSS), but uses more channels to inject code than XSS. These channels, unique to mobile devices, might be Contact, Short Message Service (SMS), Barcode, MP3, and other applications. Second, we introduce a novel tool for detecting vulnerable HTML5-based apps. We tested this tool on 15,510 PhoneGap apps collected from Google Play. Our tool flagged 478 of these apps as being vulnerable with a 2.3% false-positive rate. Last, we introduce our patching prototype that is called "NoInjection" to patch vulnerabilities of PhoneGap in Android operating system environments in order to defend and mitigate code injection attacks.

Salim El Rouayheb – Erasure Coding for Secure Cloud Storage Services; Department of Electrical and Computer Engineering, Illinois Institute of Technology

Cloud storage services allow users to store a large amount of data and enable various applications such as video streaming, social networking and file sharing. Three-times (3x) replication has been the industry standard to achieve data reliability, and to handle possible cloud storage failures. However, this solution does not scale well with the exponential increase in the data. To protect against data loss, data redundancy can be introduced either through replication or via erasure codes such as Reed-Solomon codes, as recently introduced into Facebook and Microsoft clouds. Erasure codes can achieve the same reliability levels with a lower storage cost, but can yield an increase in repair bandwidth, disk reads and latency, and can compromise security. In this talk, we propose two new families of erasure codes for cloud storage which trade off small storage overhead for savings on repair bandwidth and disk reads. On-going efforts for characterizing the fundamental limits for these tradeoffs are also described. Finally, we identify and address some of the security challenges arising from the use of erasure codes in the cloud.

Rose Gamble – Toward Increasing Awareness of Suspicious Content through Game Play; Tandy School of Computer Science, University of Tulsa

Phishing attacks occur in multiple forms, targeting content specific to the delivery modality, such as email, social media, and web browsers. These attacks sap billions of dollars annually from unsuspecting individuals while compromising information security. Though cybersecurity education should increase awareness, the average email and internet users are less attentive to media warnings and employer training materials than they are in interactive environments. Approaches to phishing awareness include test-based approaches or in-the-wild techniques, which observe user behavior by distributing faked phishing attacks. This talk proposes an improved approach that incorporates game-based learning techniques to combine the realism of in-the-wild approaches with the training features of testing approaches. The game immerses users in a role play challenge where they must send email, use social media, and browse the web, determining whether or not received content within these modalities is trustworthy. The game is implemented as a Javascript framework that simulates phishing scams, and measures trust and suspicion levels of an individual user in order to study and train that user's cybersecurity activity. The game architecture facilitates dynamic content generation for each modality, customizable experiment design for specific assessment and training, and sophisticated tracking for automated analysis of user trust content assessments. This talk overviews the game architecture and content, the specific requirements with which the game must comply, and the experimental phases.

Mina Guirguis – Stealthy Attacks on Mobile Cyber-Physical Systems: Identifying Exploits on Coordination Methods between UAVs; Department of Computer Science, Texas State University

Cyber-Physical Systems (CPSs) employing mobile nodes rely on wireless communication in many critical applications. Due to interference and intentional jamming by adversaries, mobile nodes may fail to communicate with each other causing severe performance consequences. In this talk, we present a unifying approach for identifying attacks that target Mobile CPS applications. The attack policies are obtained as solutions to Markov Decision Process (MDP) problems, in which a decision to interfere with a signal on a given link is based on the current state of the system. Through applying approximate policy iteration methods, efficient attack policies that only interfere with a selective set of signals between the mobile nodes are exposed. These policies maximize damage while minimizing exposure and detection. The proposed approach is instantiated on pheromone-based coordination methods that are used in reconnaissance, surveillance, and search missions in military operations. The identified attack policies are shown to be more potent than other attack policies including myopic, heuristic, and Denial of Service (DoS) policies.

Chin-Tser Huang – Secure Storage and Management of Big Data in Mobile Cloud Computing; Department of Computer Science and Engineering, University of South Carolina

With the fast increasing popularity of smartphones, tablets, and other mobile devices, mobile cloud computing has emerged as a significant new computing paradigm. Providing storage for individuals and enterprises has been one significant application of mobile cloud computing. However, there is one significant security risk regarding mobile cloud storage: most data systems depend on unique identifiers to distinguish different data entries. If an attacker successfully hacks into a cloud server and accesses data systems stored in it, then the attacker can get all relevant information linked to the same unique identifier. As an Air Force Summer Faculty Fellow, the PI's goal is to develop a set of schemes to enhance the security of mobile cloud big data storage and management. We currently focus on developing cryptographic shuffling algorithms and designing practical architecture for secure distribution and replication of the big data in multiple servers. Moreover, the PI also collaborates with Dr. Han to coauthor a journal paper. In the future work, we will complete the prototype implementation and evaluation, and publish a research paper of our results.

Hao Jiang – An Integrate and Fire Circuit for Reading the Memristor Crossbar Array used in Neuromorphic Computing; School of Engineering, San Francisco State University

Memristor crossbar array technology has the potential to build a highly-efficient, massively-paralleled neuromorphic computing system. Hu *et al.* collaborating with Wu and Rose in Rome Lab proposed a complete hardware design of a high-efficient neuromorphic computing using the memristor crossbar array. In, the output current from the memristor crossbar array represents the matrix vector multiplication results. Accurately sensing the output current from the memristor crossbar array is the key for the readout circuit. In, a sensing resistor is used to convert the output current into a voltage signal, then, it is amplified and digitized. A systematic error is added by including a sensing resistor. Also, having an amplifier and analog-to-digital converter for each column could significantly brings down the overall computation efficiency. During the VFRP, a high-speed integrate-and-fire circuit (IFC), which turns the current from the memristor directly into a frequency-modulated pulse train, is developed. With a digital frequency-divider or a digital counter, the IFC can facilitate both the spike-based and the level-based neuromorphic computing system. Though several IFCs were demonstrated in the past for neural networks, the IFC used here is required to operate with a very wide linear dynamic range to accommodate a large variation of the memristor resistance, ranging from 5KΩ to 5MΩ. The speed of the comparator becomes critical to ensure a large linear dynamic range. To boost its speed, a positive feedback is added in the IFC. The IFC is implemented in 0.18μm technology. Initial simulation results indicate the proposed architecture is able to readout the current from the memristor and turn it into a pulse train whose frequency is proportional to the current. It paves a way to further hardware/software development based on this high-performance computing platform.

Zhanpeng Jin – Autonomous Target Tracking On UAVS Based On Low-Power Neural Network Hardware; Department of Electrical and Computer Engineering, State University of New York at Binghamton

Detecting and identifying targets in unmanned aerial vehicle (UAV) images and videos have been a challenging problem due to various types of image distortion. Moreover, the significantly high processing overhead of existing image/video processing techniques and the limited computing resources available on UAVs make most of the processing tasks performed by the ground control station (GCS) in an off-line manner. In order to achieve fast and autonomous target identification on UAVs, it is thus imperative to investigate novel processing paradigm that can fulfill the real-time processing requirements, while fitting the size, weight, and power (SWaP) constrained environment. In this project, we present a new autonomous target identification approach on UAVs, leveraging the emerging neuromorphic hardware which is capable of massively parallel pattern recognition processing and demands only a limited level of power consumption. A proof-of-concept prototype is developed based on a micro-UAV platform (Parrot AR Drone) and the CogniMem neural network chip, for processing the video data acquired from UAV camera on the fly. The aim of this study is to demonstrate the feasibility and potential of incorporating emerging neuromorphic hardware into next-generation UAVs and their superior performance and power advantages towards the real-time, autonomous target tracking.

Ming Li – Scalable and Privacy-Preserving Searchable Cloud Data Services; Department: Computer Science, Utah State University

Cloud computing is envisioned as the next generation architecture of IT enterprises, which provides convenient remote access to massively scalable data storage and application services. Despite the cloud’s promise for huge economic savings, its benefits may not be fully realized. A wide public concern is that users’ private data may be involuntarily exposed to unauthorized parties including hackers and malicious insiders. Although end-to-end encryption has been proposed as a promising solution for secure cloud data storage, effective support of flexible data utilization such as searches over encrypted cloud data becomes a primary challenge, which is the key toward building full-fledged privacy-assured cloud data services. In this talk, we first identify the system requirements and challenges in privacy-preserving searchable outsourced cloud data services, in order to simultaneously achieve privacy assurance, scalability, and flexibility. Since these goals are often in conflict, our research aims at finding an improved solution. We also present our recent research advances in this area, beginning with a privacy-preserving multi-keyword ranked text search scheme supporting similarity-based ranking. The proposed approach integrates recent existing cryptographic primitives with information-retrieval principles and efficient data structures. A “best-effort” privacy model is adopted which achieves sublinear search time in an empirical sense. We also describe a novel way to achieve scalable and secure multi-dimensional range search. Finally, we outline some future challenges that need to be resolved to make privacy-preserving searchable cloud data service a reality.

Feng Li – Moving Target Defense Deployment in Extensible Distributed Systems; Department of Computer and Information Technology, Indiana University-Purdue University Indianapolis

The rapid change and new characteristics for the smartphone-based extensible distributed systems makes traditional collaborative defense frameworks, e.g. IDS or firewall, inefficient or ineffective. The social network properties, cloud-based information dissemination structure, and intermittent wireless communication links provide the foundation for the innovative security solutions designed for the extensible distributed systems. Many current security practices in extensible distributed systems are focusing on individual protection which makes them costly to implement and intrusive to employees, which, to some degree, negate its perceived benefits. To address such tension, we propose moving target defense deployment in extensible distributed systems. More stringent threat detection/mitigation mechanisms are deployed on selected nodes, and the node selection changes overtime. To this end, we propose a set of concepts and a distributed algorithm, to utilize the temporal-spatial pattern in an organizational environment to increase the efficiency in the security design. We present our experiment plan to make better design choices and verify the efficiency of the moving target defense design.

Xiaohua (Edward) Li – Signal Processing Oriented Big Data Privacy; Department of Electrical and Computer Engineering, State University of New York at Binghamton

This report describes our research in the 2014 Summer Visiting Faculty Research Program from May 2014 to August 2014. Our major focus is the theoretical investigation of the utility-privacy tradeoff in big data privacy. Specifically, we collaborate with Air Force to specify the big data types and big data analytic functions that this project will focus on. We develop a cloud-based big data privacy scheme that exploits both noise addition and secret transform to scramble big data. We also investigate the tradeoff between utility and privacy. As many people have recognized, the full potential of big data cannot be realized without massive data sharing. Massive data sharing not only increases the value of the data, but also triggers new data analytic techniques and applications. Nevertheless, sharing of big data faces the challenge of data privacy. The development of innovative techniques to strike the optimal tradeoff between big data privacy and big data utility is a new and critical task.

In this report, we first discuss the problems of the current research in big data privacy. Specifically, we conduct an extensive literature review of the conventional data privacy research. Although many conventional data privacy techniques have been adapted into big data applications, most of them suffer from many problems when applied to big data. To deal with this issue, we show that the extensive results in blind/non-blind channel identification developed within the community of signal processing in communications can play an important role in guaranteeing big data privacy. It is widely believed that the sheer scale of big data makes most conventional data privacy techniques ineffective for big data. In contrast to this pessimistic common belief, we propose a scheme that exploits the sheer scale to guarantee privacy. This scheme uses jointly artificial noise and secret matrix transform to scramble the source data. Desirable data utility can be supported because the noise and the transform preserve some important geometric properties of the source data. With a comprehensive privacy analysis, we use the blind/non-blind channel identification theories to show that the secret transform matrix and the source data cannot be estimated from the scrambled data. The artificial noise and the sheer scale of big data are critical for this purpose. Simulations of collaborative filtering and video surveillance are conducted to demonstrate the proposed scheme.

Rong Pan – An Analysis of Societal Sentiment and Civil Conflicts in Egypt: 2013-2014; School of Computing, Informatics and Decision Systems Engineering, Arizona State University

Utilizing the civil conflict event data recorded in the GDELT database, we analyze the group interactions among government, oppositions and populace in Egypt from April 2013 to April 2014. The societal sentiments associated with these events are extracted from the news sources that can be traced back on Internet. Time series regression models are built for four group interactions. Our results partially validate the O’Brien and Shellman’s theory on the connection between group interaction and public sentiment and the government type.

Kaliappa Ravindran – Study of Architectures for Compute-intensive Data Processing in Sensor Clouds; Department of Computer Science, The City University of New York

The summer work deals with a study of the methods and procedures for off-loading compute-intensive sensor processing tasks to the back-end cloud servers. The offloading of computations to the cloud is necessitated by the lack of adequate processing and storage resources in the field-deployed sensor devices (such as ocean-buoys and UAVs) and portable sensing devices (such as smartphones), to perform compute-intensive tasks on the raw data collected from the field. Examples of compute-intensive tasks are the image registration and feature recognition to detect objects of interest (say, using a reference image library). An application is the detection of moving objects in the border areas as part of a homeland security surveillance. Another application is the summarization of surveillance video clips of urban city regions analyzed by law enforcement agencies. Such applications are characterized by a large number of computational tasks executed by servers running on different machines for enhanced performance and information quality.

Kui Ren – Securing Emerging Short Range Wireless Communications; Department of Computer Science and Engineering, State University of New York at Buffalo

Short-range wireless communication technologies have been used in many security-sensitive smartphone applications and services such as contactless micro payment and device pairing. In this talk, we present two novel secure short-range communication systems -- SBVLC and PriWhisper. The first system, SBVLC is a secure system for barcode-based visible light communication between smartphones. As an alternative to NFC technology, 2D barcodes have been increasingly used for security-sensitive applications including payments and personal identification. However, the security of barcode-based communication in mobile applications has not been systematically studied. Due to the visual nature, 2D barcodes are subject to eavesdropping when they are displayed on the screen of a smartphone. We formally analyze the security of SBVLC based on geometric models and then propose two secure data exchange schemes. The second system, PriWhisper is a keyless secure acoustic short-range communication system tailored for smartphones. It is designed to provide a software-based solution to secure mobile communication without pre-sharing secret keys. PriWhisper explores the friendly jamming technique from radio communication for data confidentiality. The security of our proposed acoustic is analytically analyzed in terms of (in)separability of the data and jamming signals against blind signal segmentation attacks.

Alireza Seyedi – Inference in Complex Networks of Dynamical Systems; Department of Electrical Engineering and Computer Science, University of Central Florida

The problem of state estimation in a network of noisy linear time-invariant dynamical systems is considered, where the estimation is performed given observations at a subset of the network nodes. Assuming that a Kalman filter is used, an analytical upper bound is derived on the steady-state estimation error. Using this analytical bound, different approaches to select the best observation points are discussed.

Sejun Song – WiFi-Honk: Smartphone-based Beacon Stuffed WiFi Car2X-communication System for Vulnerable Road User Safety; Department of Computer Science and Electrical Engineering, University of Missouri Kansas City

As smartphones gain popularity, vulnerable road users (VRUs) are increasingly distracted by multimedia activities on their smartphones such as listening to music, watching videos, texting or making calls while walking or bicycling on the road. In spite of the development of various high-tech Car-to-Car (C2C) and Car-to-Infrastructure (C2I) communications for enhancing traffic safety, protecting such VRUs from vehicles still relies heavily on traditional sound warning methods. Furthermore, as smartphones continue to become ubiquitous, VRUs are increasingly oblivious to safety related warning sounds. A traffic accident study showed that the number of headphone-wearing VRUs involved in roadside accidents has increased by 300% in the last 10 years. Although recently a few Car2Pedestrian-communication methods have been proposed by various car manufacturers, their practical usage is limited, as they mostly require special communication devices to cope with the wide range of mobility, and also assume VRUs' active attention to the devices while walking. We propose a new smartphone-based Car2X-communication system, named WiFi-Honk, which can alert distracted VRUS of potential collisions with vehicles. WiFi-Honk provides a practical safety means for distracted VRUs without requiring any special device using smartphone WiFi. WiFi-Honk removes the WiFi association overhead using beacon stuffed WiFi communication with the geographic location, speed, and direction information of the smartphone replacing its Service set identification (SSID) while operating in WiFi Direct/Hotspot mode, and also provides an efficient collision estimation algorithm to issue appropriate warnings. Our experimental and simulation studies demonstrate that WiFi-Honk app can successfully alert VRUs within a sufficient reaction time frame, even in high mobility environments.

Video Demonstration & More Information: **IEEE Spectrum WiFi-Honk! Smartphone App Gets Pedestrians out of the Way**

http://spectrum.ieee.org/cars-that-think/transportation/safety/wifihonk-smartphone-app-for-drivers-and-pedestrians-gets-you-out-of-the-way

Venkat Venkateswaran – Enhancements To The National Operational Environment Model (NOEM) Health Module; Department of Engineering and Science, Rensselaer Polytechnic Institute

The National Operational Environment Model (NOEM) is a large scale stochastic model that recreates in software a model of any nation or region of interest. The essential attributes of the nation are captured in sufficient detail so that an analyst or decision maker can then simulate in software different intervention actions and examine their effects. NOEM will thus aid in scenario planning (stabilization, disaster recovery) and targeting. Inside the model, various modules work in concert to simulate the essential attributes of the nation. To that end there are in NOEM specific modules to simulate such facets as the nation's economy, demography, food production and critical infrastructure. The Health Module simulates the health dimension of the nation. Earlier reports, described the theory/algorithms behind the Health Module as well as the detailed tests that were carried out to verify and validate the model. The Health Module was shown to be effective in replicating in software the baseline mortality time series of a nation given a minimal set of inputs describing the nation. The model works at a granular level by constructing the mortality time series for 26 main disease groups, by gender and age groups. As we show in the report, the granularity makes it possible to model events that selectively impact certain of the disease groups, gender or age groups. This report describes two enhancements to the Health Module. These enhancements will model the added effects on the baseline mortality of specific hypothesized events. The first enhancement is a method to estimate long term radiation fatalities arising from a nuclear explosion. These long term fatalities appear in two disease groups: cancers (leukemia and solid cancers) and heart and circulatory diseases. The second enhancement provides a method for estimating excess fatalities from decrease in food production and/or water supply. Decrease in food supply will primarily result in increased fatalities in the under- 5 age group of the populace, through malnutrition. The heaviest burden from reduced water supply is on the under- 5 age group as well as the 70+ age group through diarrheal and other infectious diseases. Prototype Java versions of these models have been built and delivered to the NOEM implementation team for evaluation and inclusion in a future release of NOEM.

Shouhuai Xu – Towards Orchestrating Moving Target Defense with Quantified Mission Assurance; Department of Computer Science, University of Texas at San Antonio

Moving Target Defense (MTD) technology has been developed to enhance the resilience of cyber systems against attacks. Although there are many MTD mechanisms, there is no systematic metric to characterize the security effectiveness and sustainability of MTD. Our research uses cyber epidemic dynamics approaches to characterize and quantify the security effectiveness of MTD techniques with considerations of three classes of MTD techniques. In this talk, we introduce security metrics and an associated optimization technique that we have developed to minimize the cost of launching MTD, and to maximize effectiveness and sustainability of MTD. In addition, we discuss the results of analytic studies that we have performed to orchestrate MTD with the proposed security metrics. We conclude the talk by outlining ongoing and future research to achieve the goal for orchestrating MTD with quantified mission assurance.

Lei Yu – Improving Approximate Value Iteration with Complex Returns by Bounding; Department of Computer Science, State University of New York at Binghamton

Approximate value iteration (AVI) is a widely used technique in reinforcement learning. Most AVI methods do not take full advantage of the sequential relationship between samples within a trajectory in deriving value estimates, due to the challenges in dealing with the inherent bias and variance in the n-step returns. We propose a bounding method which uses a negatively biased but relatively low variance estimator generated from a complex return to provide a lower bound on the observed value of a traditional one-step return estimator. In addition, we develop a new Bounded FQI algorithm, which efficiently incorporates the bounding method into an AVI framework. Experiments show that our method produces more accurate value estimates than existing approaches, resulting in improved policies.

Ting Zhu – Dynamic Spectrum Allocation and Mission Control in Airborne Networks; Department of Computer Science, State University of New York at Binghamton

The demand for wireless spectrum has dramatically increased with the exponential increasing demand for services and support of different functions (communications, radar, sensors, electronic warfare, etc.) across all domains (terrestrial, aerial, and space). This demand is projected to continue growing well into the future, and will only worsen the currently felt spectrum crunch. Therefore, we have a critical need for using the spectrum efficiently via novel Dynamic Spectrum Access (DSA) techniques, which can increase the efficiency of spectrum usage by dynamically identifying the space-time-frequency vacancies (holes) and opportunistically utilizing them to benefit non-licensed entities. This type of access is also referred to as secondary access, and is expected to be implemented using Cognitive Radio (CR).

1.3. 2015 Summer Professors

Vaneet Aggarwal – Sensor Placement and Union of Subspace Completion; Department of Industrial Engineering, Purdue University.

In the first part of this work, we consider localization using multiple-input multiple-output (MIMO) systems, configured with multiple transmit and receive sensors, widely distributed in a three-dimensional space. The placement of antennas is explored, when the receive hardware has different noise quality. Cramer Rao Lower Bounds are optimized to find the antenna placements, where it is shown that a symmetric deployment of transmitting and different quality receiving sensors around the emitter is optimal.

In the second part, we extend some of the recent results on matrix completion under the assumption that the columns of the matrix can be grouped (clustered) into subspaces (not necessarily disjoint or independent). This model deviates from the typical assumption prevalent in the literature dealing with compression and recovery for big-data applications. The results have a direct bearing on the problem of subspace clustering under missing or incomplete information.

Howard A. Blair – Domain Theory of Coupled Quantum and Classical Variables with Applications to Formal Methods for Heterotic Quantum/Classical Computing; Department of Electrical Engineering and Computer Science, Syracuse University

We have developed analysis, specifically differential calculus, on continuous domains, in agreement both with differential calculus on the continuous domain of real closed and bounded intervals, situated in mainstream domain theory, and in agreement with differential calculus on convergence spaces, therefore in agreement with elementary differential calculus on Euclidean and Hilbert spaces, the latter being essential for the formal semantics of quantum programming languages. Differential calculus on such structures allows a specification logic with a rigorous mathematical semantics for formal approaches to verification of heterotic quantum/classical programs. Our previous work based on ordinary differential equations over convergence spaces needed to be extended to treat specific programming language constructs, not merely their representation as formal heterotic dynamical systems, and therefore needed to be aligned with developments in mainstream domain theory that underlays specification logics in formal methods of verification and validation. Furthermore, it has become clear that the utility and impact of the investigator's prior work on analysis on convergence spaces could be substantially enhanced by obtaining results that permitted the transfer of analytic approaches to differentiation on discrete approximations to a continuous space to the continuous space itself. Previously developed work on differential calculus on convergence spaces was specifically applied to constructing a differential calculus on the real interval domain and to differentiation of interval-valued functions of a real variable so as to provide a rigorous basis for continuous-time dependent dynamical systems with real interval-valued variables.

Soundararajan Ezekiel – Information Fusion Performance Evaluation for Motion Imagery Data using Mutual Information (initial study); Department of Computer Science, Indiana University of Pennsylvania

As technology and internet use grows at an exponential rate, video and imagery data is becoming increasingly important. Various techniques such as Wide Area Motion imagery (WAMI), Full Motion Video (FMV), and Hyperspectral Imaging (HSI) are used to collect motion data and extract relevant information. Detecting and identifying a particular object in imagery data is an important step in understanding visual imagery, such as content-based image retrieval (CBIR). Imagery data is segmented and automatically analyzed and stored in dynamic and robust database. In our system, we seek utilize image fusion methods which require quality metrics. Many Image Fusion (IF) algorithms have been proposed based on different, but only a few metrics, used to evaluate the performance of these algorithms. In this paper, we seek a robust, objective metric to evaluate the performance of IF algorithms which compares the outcome of a given algorithm to ground truth and reports several types of errors. Given the ground truth of a motion imagery data, it will compute detection failure, false alarm, precision and recall metrics, background and foreground regions statistics, as well as split and merge of foreground regions. Using the Structural Similarity Index (SSIM), Mutual Information (MI), and entropy metrics; experimental results demonstrate the effectiveness of the proposed methodology for object detection, activity exploitation, and CBIR.

Daqing Hou – Web Browser Extension Development and Data Extraction; Electrical and Computer Engineering Department, Clarkson University

This summer research project is focused on the initial research and development of the idea of “data transposition,” a term coined by AFRL’s Mr. Michael Manno, as part of the Firefox add-on called Atlas Extension

Briefly, data transposition refers to the software capability of recording the multiple manual steps involved in searching for an information item of interest using the browser, converting them into a named process, and lastly, automatically applying this created process to similar information seeking tasks in future. For example, we would like to be able to transposition from a task of finding tuition, location, and population for Clarkson University to finding the same information for St. Lawrence University or RPI. Another example would be the transpositioning of a trip planning process for the tourism destination Disneyland Hotel in CA to one for Great Wolf Lodge PA. If a transpositioned process uses the same data sources as in the recorded initial manual search, we call it a direct transposition. The college search process above would be such an example. Otherwise, it is called an indirect data transposition.

Our current focus for this summer is on direct data transposition, due to its relative simplicity. The following functionalities for supporting (direct) data transposition have been prototyped for AE as an outcome of this effort: the ability for a user to conveniently indicate those recorded steps that should belong to a process and to group them under a named process, the ability to select a named process and enact each individual step, optionally, with the ability for the user to set different values for the captured parameters, and the ability to periodically retrieve data from the data sources at a user-specified time interval. We have also conducted a preliminary experiment with a context-based approach for locating nodes of interest. Our hope is that this new approach would complement the existing path based approach and increase the robustness of AE's data location capability. A user manual and a design manual are provided to support future users and developers.

Jia (Kevin) Liu – Dynamic Control and Optimization for Airborne Networks: Fast-Convergence, Low-Delay, and Utility-Optimality; Department of Electrical and Computer Engineering, The Ohio State University

Due to the rapidly increasing mobile data demands, recent years have witnessed a large body of works on resource allocation that aim to maximize the network utility in wireless. This has led to an elegant mathematical decomposition framework, from which "loosely coupled" congestion control, scheduling, and routing algorithms naturally emerge. These algorithms do not require statistical knowledge of either the arrivals or channel states. Instead, they only rely on queue-lengths and channel state information to make control decisions. These algorithms are also inherently connected to the Lagrangian dual decomposition framework plus the subgradient method in nonlinear optimization theory [1, 2], where (scaled) queuelengths can be interpreted as Lagrangian dual variables and the queue-length updates play the role of subgradient directions.

Despite the attractive features of these queue-length-based algorithms (QLA), they suffer from several key limitations. First, in the existing QLA framework, it has been shown that a utility-optimality gap O(1=K) can be achieved with an O(K) penalty in queueing delay, where $K > 0$ is a system parameter. Hence, a small utility-optimality gap necessitates a large K and results in large queueing delay. To address this limitation, there have been significant efforts (e.g., [4, 6–8], etc.) in recent years focusing on reducing the queueing delay of these schemes (more in-depth discussions on related work later). Also, in the existing QLA framework, the queue-length-based weight adjustment ignores the curvature of the objective function contour and uses a small step-size in each iteration [1–4], which leads to unsatisfactory convergence speed. To address this problem, some second-order congestion control and routing/scheduling algorithms have recently been proposed to increase the convergence speed (see, e.g., [9, 10]). However, due to their complex algorithmic structures, these second-order approaches require a much larger information exchange overhead and do not scale well with the network size. These limitations of the existing approaches motivate us to pursue a new heavy-ball design in this paper.

More specifically, in this work, we develop a heavy-ball-based weight adjustment scheme to dramatically reduce the queue-lengths and increase the convergence speed without impacting the network utility performance and without adding any computational complexity. Our approach is based on a clever idea of separating the queue-lengths from the weights, and then uses a weight updating scheme that utilizes only one more slot of memory of the weight change in the previous time-slot. Surprisingly, we show that this simple scheme offers two control degrees of freedom that allow us to achieve utility-optimality, low-delay, as well as fast-convergence.

Venkat Venkateswaran – Critical Node Analysis (CNA) of Electrical Infrastructure Networks; Department of Mechanical Engineering, Rensselaer Polytechnic Institute

This work addresses the problem of identifying the set of nodes in a power network critical to system operation. Formally, the CNA problem is the problem of identifying a minimum cardinality set of nodes to target in a power network in order to reduce throughput by a given factor. Since the defender may reroute flows in an attempt to restore throughput, the attack must anticipate and defeat this possibility. We develop here an algorithm to solve this problem. In our approach we model the problem as a bi-level optimization problem where the master problem attempts different attack combinations and the sub-problem responds with the best routing. The optimization problems that result from such a framework are mixed integer programs (MIPs), which we solve in our Java implementation of the algorithm using CPLEX, an industry standard optimization software. The prototype has been tested on numerous benchmark problems and appears to perform well.

Meng Wang – Missing Data Recovery for Network Monitoring; Department of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute

The monitoring of Air Force information systems and networks requires the ability to accurately extract information from large volumes of measurements. Data losses often happen due to device malfunction or communication congestions. We study the missing data recovery problem for network monitoring. We exploit the low-dimensional nonlinear structures in the high-dimensional measurements and propose computationally efficient methods to recover the missing data. We also provide the theoretical analysis and numerical experiments regarding the recovery accuracy of the proposed missing data recovery method.

2. CONTINUING RESEARCH PROJECTS

2.1. 2013 Extension Grants

Bharat Bhargava – End-To-End SOA Security Protocols in Mobile Devices; Department of Computer Science, Purdue University

Service Oriented Architecture (SOA) is an architectural style that provides agility to align technical solutions to a modular business web services that are well decoupled from their consumers. This agility is extended to the Cloud model. To achieve a high level of security and a degree of decoupling whilst interoperable, SOA encourages the use of standardized transport schemes such as SOAP/HTTP(s) with Web Services (WS) family of standards specifications (commonly referred to as WS-* (WS-star)) to ease the interoperability complexity and security concerns in enterprise networks, which have medium/high bandwidth and reliable wired networks. However, these protocol standards are ill suited for mobile devices due to their limited computational capabilities, low bandwidth, and intermittent connectivity. In this chapter, we present an analysis of WS-* standards, classifying and discussing their inter-dependencies to provide a basis for end-to-end secure SOA-based cloud deployed service interactions with mobile devices. We establish an architectural consideration baseline for appropriate security mechanisms for discovering, accessing and consuming secure WS in mobile devices. We use Android smart phone to illustrate our approach.

Howard A. Blair – Computational Experiments on Filtration Schemes for Large Dynamical Simplicial Complices; Department of Electrical Engineering and Computer Science, Syracuse University

The goal of this project was to utilize the tools of computational topology to probe coarse-grained and _ne-grained structure in evolving geometric and network structures using previously developed computational topology software. Recent developments in persistent homology software - largely a matter of mathematical and algorithmic development, not merely code construction - allow to more rapidly prepare persistent homology calculations with customized filtration parameters than was previously possible creating a need for a serious study of what is possible to infer about evolving structures using these newly developed tools. Our contribution to the community of computational topology researchers with the work proposed here will be a study of a variety of filtration and multifiltration schemes for inferring the emergence, transitions occurring in, and disappearance of salient and critical properties of the evolving structures that entail the use of moderately large data sets.

Jian-Feng Cai – Linear Recovery Bound for Compressed Sensing Under Linear Transforms; Department of Mathematics, University of Iowa

In this report, we study compressed sensing of signals that are sparse under a linear transform D, which are encountered in many applications ranging from image processing to machine learning.

To sample such a signal $\_\boldsymbol{x} \in \mathrm{R}_N$ with $//D\_\boldsymbol{x}//_0 = K < N$, we use its linear measurements $\boldsymbol{b} = A\_\boldsymbol{x} + \boldsymbol{\epsilon}$, where $A \in \mathrm{R}_{M\_N}$ is a random Gaussian matrix and $//\boldsymbol{\epsilon}//_2 \leq \epsilon$ is an additive noise. Then the reconstruction $\hat{}\boldsymbol{x}$ is obtained by solving $\min_x //D\boldsymbol{x}//_1$ subject to $//A\boldsymbol{x} - \boldsymbol{b}//_2 \leq \epsilon$. In this report, we provide the theoretical guarantee of such a compressed sensing method. We will prove that the bound of the sparsity K that guarantees a stable recovery can grow linearly with respect to the number of measurements M. Compared to existing results, our bound does not depend explicitly on the condition number of D, which yields a sharper recovery bound.

Songqing Chen – Mobile Cloud Computing Case Study: Cloud, Client, and Security Challenges for Mobile Internet Streaming; Department of Computer Science, George Mason University

Mobile cloud computing applications are fast developing, thanks to the availability of cloud services and pervasive adoption of all kinds of mobile devices. Among these applications, cloud-based mobile Internet streaming services are gaining great popularity, evidenced by the dominant mobile video data traffic today. In this chapter, we first uncover the current status and challenges of existing delivery services from the perspectives of both the cloud platform and mobile devices, using a 4-month workload collected from a real-world cloud-based Internet streaming service provider and empirical experiments. On the cloud side, the device heterogeneity poses the most significant challenge for the cloud platform and effective cloud-side caching is demanded to relieve such a burden of computing-intensive transcoding. On the mobile device side, we show that different approaches have been employed by iOS and Android for streaming accesses. We elaborate through experiments how such different approaches impact the user's interests, from the aspects of the traffic amount received on and battery power consumed by mobile devices, and provide our analysis of the root cause of such differences. Furthermore, for mobile streaming applications that demand security, we discuss the application demand and how security can be offered effectively considering both the battery power constraint on mobile devices and the transcoding demand on the cloud side.

Yan Chen - Automatic Security Analysis of Android Applications with AppsPlayground; Department of Electrical Engineering and Computer Science, Northwestern University

Today’s smartphone application markets host an ever increasing number of applications. The sheer number of applications makes their review a daunting task. We propose AppsPlayground for Android, a framework that automates the analysis smartphone applications. AppsPlayground integrates multiple components comprising different detection and automatic exploration techniques for this purpose. We evaluated the system using multiple large scale and small scale experiments involving real benign and malicious applications. Our evaluation shows that AppsPlayground is quite effective at automatically detecting privacy leaks and malicious functionality in applications.

Yiran Chen – The Invisible Shield: User Classification and Authentication for Mobile Device Based on Continuous Gesture Recognition; Department of Electrical and Computer Engineering, University of Pittsburgh

Intelligent mobile devices are widely used in daily life. A large amount of sensitive information is stored on the devices, raising severe concerns regarding data security. In this work, we propose a novel user classification and authentication scheme for mobile devices based on continuous gesture recognition. The user's input patterns are collected by the integrated sensors on an Android smartphone. A learning algorithm is developed to uniquely recognize a user during their normal interaction with the device while accommodating hardware and biometric features that are constantly changing. The initial experimental results demonstrate a great possibility for our gesture-based security scheme to reach sufficient detection accuracy with an undetectable impact on user experience.

Yiran Chen – Memristor Crossbar Based Computing Engine for High Performance and Power Efficiency; Electrical and Computer Engineering Department, University of Pittsburgh

In this work, we propose a hardware realization of the Brain-State-in-a-Box (BSB) neural network model training algorithm. This method can be implemented as an analog/digital mixed-signal circuit to train memristor crossbar arrays within BSB circuits. The training effect is demonstrated through experimentation and the quality as an auto-associative memory is also ana-lyzed and compared with software based training methods. The impacts of non-ideal device characteristics and fabrication defects in crossbar arrays are discussed. Our hardware architecture shows great potential for low power, high speed, small hardware size computations, and provides inherent security features.

Yiran Chen – Robust Training Scheme for Memristor Crossbar-based Analog Neuromorphic Computing Engine; Electrical and Computer Engineering Department, University of Pittsburgh

The invention of neuromorphic computing architecture is inspired by the working mechanism of human-brain. Memristor technology revitalized neuromorphic computing system design by efficiently executing the analog Matrix-Vector multiplication on the memristor-based crossbar (MBC) structure. In this work, we propose a memristor crossbar-based embedded platform for neuromorphic computing system. A variety of neural network algorithms with threshold activation function can be easily implemented on our platform. However, programming the MBC to the target state can be very challenging due to the difficulty to real-time monitor the memristor state during the training. In this work, we quantitatively analyzed the sensitivity of the MBC programming to the process variations and input signal noise. We then proposed a noise-eliminating training method on top of a new crossbar structure to minimize the noise accumulation during the MBC training and improve the trained system performance, i.e., the pattern recall rate. A digital-assisted initialization step for MBC training is also introduced to reduce the training failure rate as well as the training time. Experimental results show that our noise-eliminating training method can improve the pattern recall rate. For the tested patterns with 128×128 pixels our technique can reduce the MBC training time by $12.6\% \sim 14.1\%$ for the same pattern recognition rate, or improve the pattern recall rate by $18.7\% \sim 36.2\%$for the same training time.

Wenliang Du – Android Security: Access Control, Attacks, and WebView; Department of Electrical Engineering and Computer Science, Syracuse University

Mobile devices, smartphones and tablets, are being adopted by many people. A recent survey shows that the global smartphone usage reached 1.5 billion at the end 2012, and it will reach 1.8 billion by the end of 2013. With such a pervasive use of mobile devices, protecting mobile systems is of critical importance. Although most mobile systems are designed with security in mind, the industry tends to be carried away by the new features that can be provided to users. It is very common that features, especially new ones, are developed without a systematic study on their security impact. In this book chapter, we first provide an overview of how access control works in Android and how some of the well-known attacks work. We then zoom in to one of the new features called WebView in mobile systems, and present its security problems, how it can be attacked, and how some of the problems can be fixed.

Soundararajan Ezekiel – An Efficient Multi-resolution Image Representation for Visual Media Reasoning (VMR); Department of Computer Science, Indiana University of Pennsylvania

In recent years, digital cameras have been widely used for image capturing. These devices are equipped in cell phones, laptops, tablets, webcams, etc. Image quality is an important characteristic for any digital image analyzing. To assess image quality for these mobile products, the original image is required as a reference image. In this case, Root Mean Square Error and Peak Signal to Noise Ratio can be used to measure the quality of the images. However, these methods are not valid if there is no reference image. In our approach, a discrete-wavelet transformation is applied to the blurred image, which decomposes into the approximate image and three detail sub-images, namely horizontal, vertical, and diagonal images. We then focus on noise-measuring the approximate images and blur-measuring the detailed images to assess the image quality. We then compute noise mean and noise ratio from the approximate images, and blur means and blur ratio from the detail co-efficient images. Further, we use a weighted scale to determine the percentage to which the image is blurred. We experimented with arbitrary weighting scales and various images, both blurred and non-blurred, and the result demonstrated the effectiveness of the algorithm. Further statistical experiments, such as R-squared statistics, need to be conducted to assign proper values to the weighting system.

Rosanne Gamble – Structuring Mobile Cloud SLAs for Matching Security Controls based on a Compliance Vocabulary; Department of Computer Science, University of Tulsa

For mission critical systems that must satisfy security constraints, the cloud introduces risks associated when cloud service providers do not implement organizationally selected security controls or policies. Mission critical information systems must be certified against a set of security controls to mitigate potential security incidents. Cloud service providers must in turn employ adequate security measures that conform to security controls expected by the organizations whose information systems they host. With service implementation details abstracted away by the cloud, organizations can only rely on service level agreements (SLAs) to assess the compliance of cloud security properties and processes. Current SLAs lack the structure, semantics, and methods needed to express and match security constraints for risk assessment when using an external cloud provider. This chapter proposes a framework, called SecAgreement (SecAg) that extends the current SLA negotiation standard, WS-Agreement, to allow security metrics to be expressed on service description terms and service level objectives. Within this framework, we demonstrate an extensible solution for building a compliance vocabulary that associates SLA terms with security controls. The terms allow services to represent those security controls which require compliance. In addition, the framework and vocabulary enable at-a-glance comparison of security service offerings so organizations can distinguish among cloud service provider compliance expectations. Using SecAg, we define and exemplify a cloud service matchmaking algorithm to allow organizations to quantify risk and identify policy compliance gaps that might exist. We assess the compatibility with existing SLAs and calculate any associated computational overhead.

Guofei Gu – SmartDroid: Automatically Revealing UI-based Trigger Conditions for Sensitive Behaviors in Android Applications; Department of Computer Science & Engineering, Texas A&M University

User interface (UI) interactions are essential to Android applications, as many Activities require UI interactions to be triggered. This kind of UI interactions could also help malicious apps to hide their sensitive behaviors (e.g., sending SMS or getting the user's device ID) from being detected by dynamic analysis tools such as TaintDroid, because simply running the app, but without proper UI interactions, will not lead to the exposure of sensitive behaviors. In this work we focus on the challenging task of triggering a certain sensitive behavior through automated UI interactions. In particular, we propose a hybrid static and dynamic analysis method to reveal UI-based trigger conditions for sensitive behaviors in Android applications. This information is very useful for analysts to (i) understand whether such behaviors are desirable for users or not (given the actual UI execution clues), and (ii) augment existing dynamic analysis tools with automatic UI interaction analysis capabilities. Our method first uses static analysis to extract expected activity switch paths by analyzing both Activity and Function Call Graphs, and then uses dynamic analysis to traverse each UI elements and explore the UI interaction paths towards the sensitive APIs. We implement a prototype system SmartDroid and show that it can automatically and efficiently analyzed the UI-based trigger conditions required to expose sensitive behaviors of several Android malware, which otherwise cannot be identified with existing techniques such as TaintDroid.

Edwin E. Hach, III – Design and Optimization of a Scalable-On-Chip Non-Linear Sign Shifter for Use in Linear Optical Quantum Computing; School of Physics and Astronomy, Rochester Institute of Technology

We present a progress report on our ongoing effort to design and optimize quantum circuits necessary for scalable, Linear Optical Quantum Computing and Quantum Information Processing (LOQC/QIP). This effort is based upon our earlier and developing theoretical advances in describing the photonic transport features of these types of circuits. The focus in this report is the analytical framework on which we base our currently in progress numerical calculations. Ultimately, we will communicate a comprehensive for scheme for the design and implementations of scalable, probabilistic devices for (LOQC/QIP).

Hai Li – Circuit Design of Memristive Switches Based Neuromorphic Computing Systems; Electrical and Computer Engineering Department, University of Pittsburgh

Memristor–the fourth basic circuit element, has shown great potential in neuromorphic circuit design for its unique synapse-like feature. However, a large gap still exists be-tween the theoretical memristor characteristics and the experimental data obtained from real device measurements. For instance, though the continuous resistance state of memristor has been expected to facilitate neuromorphic circuit designs, obtaining and maintaining an arbitrary intermediate state cannot be well controlled in nowadays memristive system. In addition, the stochastic switching behaviors have been widely ob-served. To facilitate the investigation on memristor-based hardware implementation, a stochastic behavior model of TiO_2 memristive devices based on the real experimental results was developed during my stay at AFRL in summer 2013.

During the summer faculty extension program, we continued the effort and investigated the general memristive switches based hardware implementation to better leverage the stochastic behavior of memristors. In this work, a macro cell design composed of multiple parallel connecting memristors is proposed, providing a feasible solution in memristor-based hardware implementation of neural networks. Moreover, a general memristor crossbar and associated peripheral circuitry designs have been implemented.

Chen Liu – Adaptive Virtual Machine Management in the Cloud - A Performance Counter Driven Approach; Department of Electrical and Computer Engineering, Clarkson University

The success of cloud computing technologies heavily depends on both the underlying hardware and system software support for virtualization. During our summer research, we proposed to elevate the capability of the hypervisor to monitor and manage the co-running VMs by capturing their dynamic behavior at runtime and adaptively schedule and migrating VMs across cores, in an effort to minimize the contention on system resources hence maximize the system throughput. Implemented at the hypervisor level, our proposed scheme does not require any changes or adjustments made to the VMs themselves or the applications running inside them. It also does not require any changes to existing hardware structures. These facts reduce the complexity of our approach, while at the same time improves portability. During our study in this extension period, we have successfully fortified our experimental results, showing the effectiveness of the presented approach in improving the overall system throughput when comparing against default management scheme, especially in a multi-core multi-threading scenario, which is commonly deployed in cloud-computing platforms.

Lingjia Liu – Technical Report: Throughput Optimization in Sensing-Based Dynamic Spectrum Access Networks With Rate Loss Constraint; Department of Electrical Engineering and Computer Science, University of Kansas

Dynamic spectrum access (DSA) has been regarded as one of the key techniques to improve the spectral efficiency of a wireless communication network. The basic idea of DSA is to allow the unlicensed user or Secondary User (SU) to use licensed user's or Primary User's (PU) spectrum under the condition that SUs do not cause harmful interference to PUs. Based on the difference on SU's access to PU's spectrum, DSA can be divided into two paradigms: overlay and underlay. In overlay systems, SU will first do spectrum sensing, and if SU senses PU idle, SU will use this idle spectrum; otherwise, SU will keep silence on this active spectrum. In underlay systems (spectrum sharing), SU accesses to PU's spectrum no matter PU is active or not, but at a low power in order to guarantee that SUs interference to PU does not exceed one threshold.

Recently, one new criteria called PU Rate Loss Constraint (RLC) has been proposed. Rate Loss Constraint means that PU's maximum rate loss due to SU's transmission should not exceed a threshold. This shows that compared to traditional Interference Power Constraint (IPC), SU can achieve a higher transmission rate under RLC. In this technique report, we extend RLC to sensing based dynamic spectrum access network. Sensing based DSA is SU's new access paradigm in CR proposed by and the main idea is that SU will first do spectrum sensing. If SU senses that PU is idle, SU will transmit at a high power, otherwise, SU will transmit at a low power. With RLC, SU should control its power and guarantee that PU's rate loss under a meaningful threshold. We can see that SU will transmit without considering the interference threshold constraint during PU is idle and transmit at a low power subject to satisfying the PU rate loss constraint. Therefore, this sensing based dynamic spectrum access network can improve SU's throughput significantly since it combine the advantage of overlay and underlay.

Nicholas Mastronarde – Scheduling Heterogeneous Flows Over a Bottleneck Airborne Network Node; Department of Electrical Engineering, University at Buffalo

We formulate the problem of optimal scheduling at a congested bottleneck Airborne Network node as a Markov decision process (MDP) that considers the dead lines and priorities of each packet as well as the dynamic packet arrivals and channel conditions. Within this framework, we consider two scheduling problem formulations with the same objective but different constraints. In the first formulation, the objective of the MDP is to maximize the congested node's long-run utility (i.e., priority-weighted throughput) subject to a long-run cost constraint (i.e., energy consumption). In the second formulation, the objective is to maximize the congested node's priority-weighted throughput subject to instantaneous transmission rate constraints. In this report, we discuss these problems' key challenges, and analyze the structural properties of the optimal scheduling policy with respect to the deadlines and priorities of the backlogged packets, and provide some preliminary experimental results showing the benefits of the proposed approach.

Jing Peng – Combining the advice of Experts with Randomized Boosting for Robust Data Fusion; Computer Science Department, Montclair State University

We have developed an algorithm, called ShareBoost, for combining mulitple classifiers from multiple information sources. The algorithm offer a number of advantages, such as increased confidence in decision-making, resulting from combined complementary data, good performance against noise, and the ability to exploit interplay between sensor subspaces. We have also developed a randomized version of ShareBoost, called rShareBoost, by casting ShareBoost within an adversarial multi-armed bandit framework. This in turn allows us to show rShareBoost is efficient and convergent. Both algorithms have shown promise in a number of applications.

The hallmark of these algorithms is a set of strategies for mining and exploiting the most informative sensor sources for a given situation. These strategies are computations performed by the algorithms. In this paper, we propose to consider strategies as advice given to an algorithm by “experts” or “Oracle.” Note that we make no assumption regarding the generation of the advice. In the context of pattern recognition, there may be several pattern recognition strategies. Each strategy makes different assumptions regarding the fidelity of each sensor source and uses different data to arrive at its estimates. Each strategy may place different trust in a sensor at different times, and each may be better in different situations. In this paper, we introduce a novel algorithm for combining the advice of the experts to achieve pattern recognition performance, close to the best expert. We show that with high probability the algorithm seeks out the advice of the experts from decision relevant information sources for making optimal predictions. Finally, we provide experimental results using face and infrared image data that corroborate our theoretical analysis.

Indrajit Ray – Access Control in Mobile Clouds Balancing Security, Cost and Functionality; Access Control in Mobile Clouds Balancing Security, Cost and Functionality

Ensuring proper access control within mobile clouds requires identifying how to deploy, where to deploy, and how to manage the access control components. It is very difficult to achieve the traditional monolithic reference-monitor model of access control within a mobile cloud setup together with the tamper-proof property required of the trusted computing base implementing the reference-monitor. Authorization and access control, consequently, need to be implemented as a composition of many smaller reference monitors and deployed in a distributed and elastic manner. There are clear tradeoffs between the security achieved, cost accrued and functionality penalties incurred with this alternative approach. This chapter investigates models and algorithms to best deploy access control in mobile clouds, balancing security, cost and functionality in the process.

Indrakshi Ray – Real-Time Auditing in Mobile Clouds; Department of Computer Science, Colorado State University

With the ever-increasing use of cloud to provide services, real-time auditing becomes critical to monitor attacks and safeguard these services. Audit log streams that are being generated by these services continuously can be monitored by using a data stream management system and appropriate actions can be taken when events of interest happen. Audit log streams are generated at different nodes. It is important to process such streams in an efficient and secure manner. The problem becomes even more complex for a mobile cloud, where the availability of the nodes and their mobility impact query processing. Towards this end, we discuss a secure information flow model for processing audit data, which protects against sensitive information leakage and also describe the issues that need to be considered for efficiently processing audit streams generated in a mobile cloud.

Jian Ren – Mobile Cloud Computing: Architecture, Applications, and Security - An Introspective View; Department of Electrical & Computer Engineering, Michigan State University

Mobile cloud computing (MCC) is emerging as a new computing paradigm and has recently attracted significant attention and interest both academia and industry. The scope of applications for MCC has extended far beyond offloading of computing cycles and battery energy. In this book chapter, we attempt to present a survey of MCC from the perspective of its intended usages and security challenges. Specifically, we introduce three common mobile cloud architecture components. We classify the comprehensive existing MCC applications into two fundamental categories: computation offloading and capability extending. Considering the energy bottleneck and user context of mobile devices, we discuss the research challenges and opportunities of introducing cloud computing to assist mobile devices, including energy-efficient interactions, virtual machine migration overhead, privacy, and security. Moreover, we demonstrate real-world applications enabled by mobile cloud computing in order to stimulate further discussion and development of this emerging field.

Sejun Song – Component-Oriented Data Encryption and Deduplication for Mobile Cloud Computing; Department of Computer Science and Electrical Engineering, University of Missouri-Kansas City

As smartphones gain their popularity and the usage applications become versatile, smartphone users are also hoping to perform resource intensive tasks at anywhere and anytime as conveniently as using their static computers. To overcome the smartphone's intrinsic resource limitations, emerging Mobile Cloud Computing (MCC) augments the smartphone's processing and storage capabilities by leveraging cloud distributed resources. However, the demand of greater data exchange among the devices within MCC is considered as a significant performance bottleneck. An efficient technique to reduce and secure data at a source is essential to save network bandwidth from a user to cloud servers or storage spaces. It, in turn, expedites the data transmission speed as well as reduces vulnerability of data movement among MCC platforms. Although traditional variable-size block-level data deduplication techniques along with compression methods tend to achieve a high data reduction rate, they require high processing overhead due to data chunking, index processing, and data fragmentation. However, a smartphone can be limited in processing capability and memory space to perform an effective client side deduplication. While, a simple file-level or a large fixed-size block-level deduplication may be able to cope with the limited source device capacity, it cannot produce a high data reduction rate. In this project, we design and develop a novel Component-Oriented Data Encryption and Deduplication (CODED) mobile application that achieves both fast and effective data encryption and reduction for MCC services. Specifically, CODED efficiently deduplicates redundant objects in files, emails, as well as images exploiting object-level components based on their structures. It also effectively reduces the overall encryption overhead on the mobile devices by adaptively applying compression and encryption methods according to the decomposed data types. Our evaluation using real datasets of structured files and emails show that the proposed scheme accomplishes as good storage savings as a variable-block deduplication, while being as fast as a file-level or a large fixed-size block-level deduplication.

Alex Sprintson – Applications of Network Coding for Securing Mobile Cloud Data Storage; Department of Electrical and Computer Engineering, Texas A&M University

Mobile cloud computing systems are inherently dynamic due to the mobility, user churn, and limited power supply. Due to their ubiquitous deployment, such systems are also vulnerable to malicious attacks. Accordingly, design of reliable and secure mobile could computing systems has attracted a significant attention from the research community.

Data layer a key component of the mobile cloud computing systems. The key functions of the data layer include data storage, data dissemination, error control, and data protection. The main challenge in this context is to ensure efficient, robust, and secure operations of the data layer in the presence of unreliable wireless channels, packet loss, eavesdroppers, and malicious users. In this chapter we show how to leverage the network coding techniques to ensure the reliability and robustness of the systems.

We show several important advantages of the network coding techniques in this context. First, we present a coding schemes that protects the data stored at the mobile cloud from an adversary who is able to get access to one device. Second, we describe a coding scheme that protects the data from and eavesdropper, i.e., a malicious node that observes the data transmitted over the broadcast channel. Finally, we discuss the case in which an adversary can modify the data at the devices.

Dmitry Uskov – Photonic Quantum Information Processing: Beyond the "Qubit" Paradigm of Quantum Computation; Department of Mathematics and Science, Brescia University

We performed a theoretical research focused on developing robust and scalable methods and technology in quantum optical information computing. We have developed mathematical tools based on geometric properties of multidimensional Lie Group manifolds aiming at exploiting super-exponential scaling of the dimensionality of photonic Hilbert space. As we have discovered recently, when the number of optical modes and photons increase optical quantum computation offers much better scaling of available quantum resources than traditional schemes based on an abstract notion of elementary carrier of quantum information, aka "qubit". Our recent research has achieved considerable progress in numerical methods of designing efficient linear optical quantum transformations and there was a considerable lag in developing analytical tools for analysis of the numerical results. Therefore present work is completely dedicated to designing and developing analytical methods based on Lie Group theory. Specifically we focus on i) physical analysis of multipartite entanglement using Plucker coordinates for SU group and ii) geometric analysis of holonomic quantum computation using Konstant-Kirillov-Sourian 2-form extension of non-Abelian phase. The current state of the work is outlined below in two sections drafted for future publication in New Journal of Physics and Journal of Physics A**.**

Kaiqi Xiong – Approaches for Securely Locating Cloud Data; Department of Computing Security, Rochester Institute of Technology

As predicted, the market for cloud-based mobile applications will reach over $10 billion by 2015. More and more are shifted to the cloud for computation and storage due to the limited capacity of mobile devices. Thus, the location-aware security and performance assessment of mobile services plays an important role in mobile cloud computing (MCC). On one hand, understanding the end-to-end security and performance of mobile services becomes necessary for the successful deliver of MCC services. One other hand, the accuracy of data location information is critical for many MCC applications, especially those used in open network environments where malicious adversaries may disrupt and change the data communications between mobile-users and cloud providers. It is impractical to assume that all cloud providers are trustable and all data communications are not altered. Most of the existing GEO-location discovery schemes can only be used in the trusted environment. In this chapter, we propose approaches for assessing the security and performance of mobile services and securely locating the location of mobile data. We have conducted simulations to analyze the performance of the proposed approaches.

Kai Zeng – Multipath Physical Layer Authentication in Multihop Wireless Networks; Department Of Computer And Information Science, University Of Michigan – Dearborn

Exploiting physical layer characteristics to enhance or complement authentication strength in wireless networks has been attracting significant research attentions in recent years. Previous works on physical layer authentication mainly focus on single-link or single-path communication. In this paper, we propose a physical layer multipath challenge-response authentication mechanism (PHY-MPA) for multihop wireless networks. PHY-MPA exploits randomness, coherence, and location decorrelation properties of the wireless fading channel to securely convey the product of the channel state information on consecutive links and use the fading channel to encrypt challenge and response messages. The challenge and response messages are transmitted via multiple paths to improve the successful authentication rate under low SNR. PHY-MPA is immune to both outside and inside attacks with an untrusted relay. PHY-MPA adopts the orthogonal frequency division multiplexing (OFDM) technique to modulate the authentication key and challenge-response messages on subcarriers. Physical layer pilots and preambles are eliminated to prevent an attacker from gaining knowledge about the channel state information, and as a result prevent the authentication key from being revealed to untrusted attackers. We analyze the security strength of PHY-MPA and conduct extensive simulations to evaluate its performance. It shows that PHY-MPA can achieve both high successful authentication rate and low false acceptance rate, and improve the performance of single-path authentication.

Ming Zhao – Cross-layer Optimization for Virtual Machine Resource Management in Mobile Cloud; School of Computing and Information Sciences, Florida International University

Virtualized systems (e.g., public and private clouds) are playing an increasingly vital role to support the computing of applications from different domains, including the emerging applications on mobile computing platforms (e.g., smartphones, tablets). Existing resource management solutions in such systems typically treat virtual machines (VMs) as black boxes, which presents a hurdle to achieving application-desired Quality of Service (QoS). This report advocates the cooperation between VM host- and guest-layer schedulers for optimizing the resource management and application performance. It presents an approach to such cross-layer optimization upon fuzzy-modeling-based resource management. This approach enables the host-layer scheduler to feedback resource allocation decisions and adapt guest-layer application configurations. As a case study, the proposed approach is applied to map services which are widely used by mobile applications and have challenging dynamic, complex resource demands and sophisticated configurations. Specifically, for map services, the proposed approach adapts the quality of returned map imagery in order to meet the response time target as the workload intensity and available network bandwidth change over time. A prototype of the proposed approach is implemented on Hyper-V VMs, and evaluated using real workloads collected from TerraFly, a production map service. The results show that with the proposed host-to-guest application adaptation, the performance of the TerraFly workloads is improved by 15% in response time and 40% in map imagery quality, compared to schemes without adaptation.

2.2. 2014 Extension Grants

Sanjukta Bhowmick – Simulation Interface For Large-Scale Testing of the Bio-AI Project; Computer Science Department, University of Nebraska at Omaha

The goal of this project was to develop a simulation interface for testing the deployment of multiple UAVs using the BIO-AI simulation method. The interface would be used to test different robustness conditions as well as possible error conditions that can occur in creating robust tentacles (or pathways) of UAVs between the source and destination.

Our original goal was to have one student devoted completely to working on the code and another to research on different graph theory aspects. However, our co-ordinator in the project, Bo Ryu, insisted that the code should be written only by U.S. citizens/permanent residents. This created an issue in execution of the original plan, since most graduate students applying to computer science are international students. After discussion, we decided that the international student would research on the swarming behavior of robots as a precursor to adding that component into the BIO-AI simulation, while the code would be written partially by me until I find a qualified student who was an U.S. citizen. I was successful in finding such a student (he is an undergraduate who is joining our graduate program next year) around mid November and he has made considerable progress in the code since then. This report therefore contains two parts: (i) The BIO-AI simulation code and (ii) Overview of papers on different swarming models.

The BIO-AI Simulation Code: During this Fall, we have extensively refactored the original code given in [1] to handle multiple UAVs and to efficiently transmit the positions of the UAVs to their neighbors. Currently the simulator successfully handles multiple UAVs, and creates tentacles of UAVS from a specified source to destination. The UAVs are launched one at a time. Once a UAV reaches its position, the next UAV is launched. The simulation can support multiple sources, destinations as well as the creation of multiple tentacles.

The BIO-AI simulation code and (ii) Overview of papers on different swarming models.Howard A. Blair – Heterotic Quantum Dynamical Systems; Department of Electrical Engineering and Computer Science Syracuse University

The prior work of the PI and his graduate students allow for extending Abramsky's Quantum Programming Language to have dynamic unitary qubit operations and concurrent execution of the language's commands. It is trivial to extend the language's syntax; the real issue, upon which verification and strong validation depends going forward, is *the goal of this project: to provide a rigorous mathematical semantics with respect to which formal methods of program verification can be developed*.

The problems associated with this have solutions ready-made based on the prior work of the PI and his graduate students and that this prior work will lend itself to two of the problems associated with constructing the underlying mathematical semantics of Abramsky's language are (1) factoring state evolution laws (these would be the control laws in a classical control-of-plant scenario) across potentially entangled qubits, and more importantly (2) to organize a *specification logic* for heterotic quantum/classical dynamical systems. A specification logic gives a means of formally expressing that a state evolution of a state takes place from a *precondition* region within a space of states to a *postcondition* region, and the logic gives as well a means of expressing formally rigorous computably checkable proofs of assertions about the state evolution.

Upendranatha (Sharma) Chakravarthy – Stream Processing Framework for Expressing Situational Awareness, Department of Computer and Computational Sciences, University of Texas at Arlington

Complex event Processing (CEP) has come a long way (since the Eighties) from adding simple monitoring capabilities – in the form of triggers – to Database Management Systems (termed active DBMSs) to process continuous, varying input rate data and event streams from sensors and other applications (e.g., UAVs). The requirements as well as the capabilities needed for newer applications have changed drastically from its beginnings. Many event specification languages, optimization techniques for processing live as well as collected data (termed event logs in the event processing community and forensics in the video processing community, respectively) have been developed. Distributed applications have additional issues on computation distribution, fault-tolerance, and recovery aspects of CEP.

Stream processing (SP) became relevant mainly due to inexpensive and hence ubiquitous deployment of sensors in many applications (e.g., environmental monitoring, battle field monitoring). Other continuous data generators (web clicks, traffic data, network packets, mobile devices) have also prompted processing and analysis of these streams for applications such as traffic congestion/accidents, network intrusion detection, and personalized marketing.

Although SP and CEP are used in many diverse application domains, surprisingly, *these technologies have not been exploited for video analysis and fusion* to the best of our knowledge. Situation awareness requires, collecting, aggregating, and analyzing disparate data types (e.g., video, sensor, audio, call reports) in order to make informed decisions. If it is a realtime or near real-time decision making (surveillance as compared to forensics where archived data is analyzed), additional real-time processing and interactive requirements become critical. Video analysis and extraction of relevant content characteristics are also processing-intensive and requires computations that are very different from those used on categorical and numeric data. Moreover, modeling of complex situations using events and aggregation of components of video analysis is not straightforward. As a result, video analysis and fusion has focused on customized solutions for specific problems (e.g., object identification, object classification, overlaps of objects, tracking object movements.) A large number of techniques (both pattern recognition-based and machine learning-based) for processing video frames to characterize objects have been developed to deal with camera angles, lighting effects, color differences, as well as object identification and re-identification. Feature extraction, segmentation, and separation of background from foreground use numerous algorithms and machine learning techniques to deal with specific application domains. Also, the input quality and characteristics vary quite significantly among video streams (based on frame rate, pixel density, and appliances used, etc.) which necessitates the use of specific algorithms and approaches. Of course, the image processing technology is continuously improving as also the collection technology.

The focus of this work is to evaluate the applicability of stream and complex event processing techniques to video analysis and fusion applications with the intent of leading to alternative, high-level specification of situations, their mapping to well-defined lower level operators and their computation, optimization, and subsequently reasoning about quality of service (QoS), capacity modeling, as well as parallelization. The higher-level specification will also help in translating or mapping general situations (e.g., track an object where the object can be specified as a parameter) into their corresponding computations.

Mainak Chatterjee – Reliability of Distributed Systems Under Imperfect Monitoring; Department of Electrical Engineering and Computer Science, University of Central Florida

Reliability of cooperative decision mechanisms is critical for the proper and accurate functioning of a networked decision system. However, adversaries may choose to compromise the inputs from different sets of components that comprise the system. Often times, the monitoring mechanisms fail to accurately detect compromised inputs; hence cannot categorize all inputs into polarized decisions: compromised or not compromised.

In this project, we propose a Bayesian inference model based on multinomial evidence to quantify reliability for a cooperative decision process as a function of beliefs associated with observations from the imperfect monitoring mechanism. We propose two reliability models: an optimistic one for a normal system and a conservative one for a mission critical system. We also provide an entropy measure that reflects the certainty or uncertainty on the calculated reliability of the decision process. Through simulation, we show how the reliability and its corresponding entropy changes as the accuracy of the underlying monitoring mechanism improves.

Yuejie Chi – One-bit Principal Component Analysis; Electrical and Computer Engineering Department, Ohio State University

This work proposes a simple sensing and estimation framework to faithfully recover and track the principal subspace of a data stream from a collection of one-bit measurements from distributed sensors. The framework is motivated from decentralized networked sensing applications, where the sensors may be computationally and bandwidth-constrained to communicate at high data rates. The one-bit measurements are comparison outcomes between energy projections of the covariance matrix over pairs of random directions. By leveraging low-dimensional structures, the top eigenvectors of a properly designed surrogate matrix is shown to recover the principal subspace as soon as the number of bit measurements exceeds certain threshold. The sample complexity to obtain reliable comparison outcomes is also obtained. When the measurements arrive sequentially over time, we further develop a low-complexity algorithm to track the principal subspace.

Soundararajan Ezekiel – No-Reference Multi-scale De-blurring, De-noising, Polarimetric Analysis & Advanced Fusion Performance Evaluation Tool for VMR/CBIR; Computer Science Department, Indiana University of Pennsylvania

In the past decade the popularity of digital cameras has increased many fold and the most common problem in digital image are Noises and Blur which degrade the quality of the photography. When you use camera, you want to capture the scene as close to as it is that represent the scenes in more realistic as it appear for us. All images are mostly blurry due to the following reasons: lenses are not perfect, camera lenses may be out of focus, object movement, and in general the light may smeared out and scene information is spilled over neighboring pixels. It is very difficult to avoid noise and blur and these two will destroy the scene quality. Deblurring and denoising got lots of attention in image processing communities specifically computer graphics and machine vision. Denoising is a process that is used to remove unwanted disturbances from an image and hence it is ohen necessary and an important first step for any image analysis. Over the years there is number of denoising algorithms has been developed. These algorithms are depending on type of image and the noise characteristics (Gaussian, Salt and Pepper, speckle etc.) can be grouped as two categories:

A. Spatial domain Filtering
    - Linear Filtering: It is a basic approach: Gaussian, Weiner, Mean filtering methods but these approaches have tendency to over smoothing edges and remove image details
    - Non Linear filtering: Median, weighted median, spatial median methods employs low pass filters with an assumption that noises are located in higher frequency regions of images. These methods do remove noises but blur the images a lot.
B. Transform domain: It is Statistically Based Approaches- Bilateral filtering, antistrophic diffusion, wavelet based methods uses more sophisticated methods that uses image statistics that enhance large intensity edges and suppress low intensity edges. Deblurring is the process of making images that represent the scene as we see it which makes image more realistic, sharp and more useful for further analysis and image processing. That is recovering original scene from image using mathematical model. In this process, some information will be lost and this can be recovered only if you know the deblurring process. Even though, we may not be able to recover fully the original image because of various errors such as: hardware problem, truncation and approximation. Deblurring process is

difficult problem because the observed blurred image provides only partial constraints with infinitely many blur kernels. Further, if we have finite number of blur kernel or known blur kernel, we could have infinite number of original sharp image to convolute which makes harder to develop appropriate algorithm. Deblurring is a very important image processing step because it has lot of important application in various fields such as medical imaging, astronomical imaging, and visual media representation, context based image retrieval.

The main focus of our proposal is to first define a general model such as Riemannian Manifold and explore several Multiscale decomposition techniques with the following important properties:

- Multiscale decomposition
- Directional decomposition, Perfect reconstruction
- Fixed Transformation with low redundancy
- Sparse representation for images with smooth curves

Outcome of this goal is two papers that have been completed and presented to the following conference:

1. ***Modified De-convolution using Wove/et Image Fusion:*** 2014 Applied Imagery Pattern Recognition (AIPR), Washington DC, October 14-16, 2014 (Refer Appendix A for the full paper)
2. ***Multi-resolution Deblurring:*** 2014 Applied Imagery Pattern Recognition (AIPR), Washington DC, October 14-16, 2014 (Refer Appendix A for the full paper)

Aram Galstyan – Understanding Network Dynamics via Correlation Explanation; Computer Science and Information Sciences Institute, University of Southern California

Recent proliferation of various sensing devices has resulted in a large amount of multivariate and multi-modal data describing dynamics of various complex systems such as heterogeneous information networks. Analyzing such data is vital for understanding network operations and predicting its future behavior. Extracting actionable knowledge from such high dimensional data, however, can be an extremely challenging problem due to a number of reasons. First of all, the number of measured variables can be in hundreds or even thousands, while the number of data points can be relatively small compared to the overall size of the state space. Second, each measured variable individually will be a very week predictor of the system's true state and its dynamics, so that one needs to aggregate "signals" from different covariates in order to infer the current state and predict the dynamical evolution of the systems. In fact, many (most) of those variables might be completely irrelevant for assessing the true state of the network. And finally, not all the measurements are available all the time, which necessitates a method that is robust to missing data.

Edwin E. Hach, III – Applications of Scalable Linear Optical Networks for On-Chip Quantum Information Processing and Metrology (Ring Resonator Work) and Entanglement Generation and Characterization in Continuous Variable Quantum Optical Systems (Bell Inequality Work); Department of Physics and Astronomy, Rochester Institute of Technology

I present a progress report on two active areas of our ongoing collaboration. First, I review the status of our calculations demonstrating violations of a Bell inequality by SU Parity Entangled Perelomov Coherent States of a bimodal quantum mechanical system. Second, I give a status update, including new results, of our theoretical work on linear quantum information processing using silicon nanophotonic ring resonators.

Hao Jiang – Power/Area Efficient Readout Circuit for Memristor Crossbar Array Based Neuromorphic System; Engineering Department, San Francisco State University

The neuromorphic system has the potential to be widely used in a high-efficiency artificial intelligence system. Simulation results have indicated that the memristor crossbar array has the potential to configure a massively-paralleled neuromorphic system. In a memristor crossbar array based neuromorphic system, one readout circuit is required for each column in the memristor crossbar array. The current approach involves an op-amp based readout circuit, and, another op-amp based integrate-and fire circuit for the spike-based design, or an analog-to-digital converter for the level-based design [2]. The power consumption and the needed chip area of the aforementioned readout circuit prevent it to be used in a massive parallel neuromorphic system. An innovative high-speed integrate-and-fire circuit (HIFC) has been proposed during the VFRP. The new architecture only involves a low-value (*i.e*., small size) capacitor, a comparator and a digital counter. Potentially, the new architecture is able to achieve high speed, low power and small area at the same time. During the extension study, the proposed H-IFC has been implemented in IBM 0.13⌠m technology. The H-IFC has successfully converted the input current into a frequency-modulated pulse train. The linearity of the conversion is ultimately limited by the comparator’s area and the power consumption.

Taylor T. Johnson – Inferring Physical System Specifications from Embedded Software Tests; Computer Science and Engineering, University of Texas at Arlington

Embedded systems use increasingly complex software and are evolving into cyber-physical systems (CPS) with sophisticated interaction and coupling between physical and computational processes. Many CPS operate in safety-critical environments and have stringent certi_cation, reliability, and correctness requirements. These systems often undergo changes throughout their lifetimes, where either the software or physical hardware is updated in subsequent design iterations. One source of failure in safety-critical CPS is when there are unstated assumptions in either the physical or cyber parts of the system, and new components do not match those assumptions. In this work, we present an automated method towards identifying unstated assumptions in CPS. Dynamic specifications in the form of candidate invariants of both the software and physical components are identified using dynamic analysis (executing and/or simulating the system implementation or model thereof). A prototype tool called Hynger (for Hybrid iNvariant GEneratoR) was developed that instruments Simulink/Stateow (SLSF) model diagrams to generate traces in the input format compatible with the Daikon invariant inference tool, which has been extensively applied to software systems. Hynger, in conjunction with Daikon, is able to detect candidate invariants of several CPS case studies. We use the running example of a DC-to-DC power converter, and demonstrate that Hynger can detect a specification mismatch where a tolerance assumed by the software is violated due to a plant change.

Dhireesha Kudithipudi – Computational Architecture of the Echo state Networks For Speech Emotion Recognition; Computer Engineering Department, Rochester Institute of Technology

Echo state neural networks (ESNs) provide an efficient classification technique for spatiotemporal signals. The feedback connections in the ESN topology enable feature extraction in both spatial and temporal components in time series data. This property has been used in several application domains such as image and video analysis, anomaly detection, and speech recognition. In this research, we explore the hardware architecture for realizing ESN efficiency in power-constrained devices. Specifically, we propose a scalable computational architecture applied in speech-emotion recognition. Two different topologies are explored, with underlying core memory as memristive synapses. The simulation results are promising with a classification accuracy of ≈ 96% for two distinct emotion statuses ≈ 96% for two distinct emotion statuses.

Sunil Kumar – Design of Wireless Protocols for Links with Multiple-Beam Smart Antennas; Electrical and Computer Engineering Department, San Diego State University

To support growing warfighter needs, the next generation of airborne data links and networks will need to provide higher capacity, longer range, greater flexibility, faster response times, and increased interoperability between diverse systems. Although the concept of modularity is a foundation of the current Internet, the air tactical domain has embraced a tightly coupled, vertically integrated architecture for increasing efficiency. Future airborne networks can benefits from a hierarchical, modular architecture similar to that of the Internet to knit together various heterogeneous systems. The airborne networks have several unique characteristics, including limited spectrum, high mobility and adversarial environment, high data rates and low latency constraints, long transmission ranges, and significant multicast traffic. These impact each network layer and therefore need to be considered in the design of protocols.

The challenge in military networks is to organize a *reliable* wireless network in the presence of dynamic topology, heterogeneous nodes, directional and intermittent links, and dynamic spectrum allocation. The mission-aware information representation and QoS-aware cross-layer network protocols are *key enablers* in effectively deploying the military network infrastructure. We focus on the design of cross-layer protocols that have the potential to provide large improvements in network connectivity, capacity and interoperability for AN. Development of efficient MAC protocols can improve bandwidth efficiency and reduce latency. Routing schemes can enhance multi-hop reachability for longer range configuration, ease of configuration and topology management, and avoid or reduce the effect of jamming.

There is a growing interest in the use of multiple beam smart antennas (MBSA) (capable of adaptively configuring multiple narrow beams and nulls) for enabling multiple simultaneous directional transmissions using the same channel, supporting large data rates and transmission ranges, interference avoidance, and AJ by null formation in the direction of jam. A single beam antenna also offers spatial reuse, but it allows only one transmission or reception by node at a given time. However, the use of directional antenna (*i*) requires the design of neighbor and topology discovery techniques for mobile nodes; (*ii*) introduces new hidden node problem due to node deafness; (*iii*) requires distributed scheduling schemes to avoid performance degradation due to hidden nodes. Since antenna direction also impacts the routing path, a cross-layer design among routing-MAC-PHY is required.

Although several protocols exist for a single beam directional antenna, there has been relatively little work on the protocols for MBSA in the literature. Since MAC layer plays a very important role in leveraging the benefits of MBSA, it needs to be properly designed. Furthermore, most protocols in the literature assume half-duplex links which impose many restrictions on the protocols. There is a need to investigate the fundamental issues for the design of cross-layer MAC and routing protocols for MBSA with full-duplex links using a single channel, especially because the common data link (CDL) for military communication uses the full-duplex transmission. To the best of our knowledge, the use of full-duplex links with MBSA has not been studied in academic literature so far.

This report describes different types of mission data and issues related to defining a network utility function, followed by the issues in the design of a cross-layer MAC and routing layer protocols for multiple beam smart antennas.

Qi Liao – Large-scale Network Anomaly Analysis Using Dynamic Graph Mining and Visualization; Department of Computer Science, Central Michigan University

The analytic complexity of networks has been increasingly challenging over the past decades due to the ever growing size of networks and the explosion of information exchanged over the Internet, known as the *big data* era. Large-scale networks could suffer from threats from all aspects. How are we going to separate the abnormal (or potentially bad) traffic from the normal traffic despite the noisy nature inherent with security datasets? The abnormal activities, to which we refer as anomalies, may be related to faulty hardware/software, misconfiguration, or security related events caused by malicious users and applications. While there has been effort in anomaly-based intrusion detection, the detection of abnormal and potentially malicious *connections* has remained challenging. Anomaly analysis is extremely useful in many domains, for example, network managers and administrators need to monitor the latest traffic graphs to increase *situation awareness* for both effective troubleshooting and time-efficient security-related investigation.

We study how to effectively detect, and more importantly analyze the underlying causes of, anomalous network connections and health situations of networked systems. Our approach is based on two important features of network log data, i.e., the topological structures such as information from network flow data, and the health attributes of systems such as connectivity, CPU, disk, memory, etc. For better defense against the increasing zero-day attacks, we aim to utilize behavior or learning based approaches, in particular, link prediction algorithms to analyze network connections. The challenges lie in a few key characteristics of anomaly detection that are fundamentally different from link prediction tasks. Although link prediction, may predict whether a pair of nodes that have not been connected in the past will ever be connected sometime in the future, it does not consider pairs of nodes that have previously been connected. It has been observed that networks are not only becoming much larger but much more heterogenous, complex and dynamic as well. The fundamental deficiency of traditional link predictions is that they do not consider the *dynamics* of network connections, e.g., the on/off patterns. Taking computer networks for example, the massive amount of traffic among the computing nodes is constantly changing, e.g., users and applications may come and go at any time, establishing and tearing down the connections.

The contribution of our research study is twofold. First, we developed link anomaly scoring and link anomaly detection algorithms for dynamic network graphs. Second, we developed a web-based network anomaly visualization framework that allows a network operator to explore and investigate the inter-relationships and underlying causes of network anomaly events. To keep the algorithms generic, our link anomaly detection algorithms does not require additional information such as node attributes, but is purely based on the network topologies. To solve the aforementioned challenges, we build our approaches on the dynamic graph structures by including a time dynamic function and similarity measurement based on the evolving network topologies in consecutive time windows. Intuitively, the frequency of links' appearances implies the importance of such connections. It is reasonable to assume that the connections close to the time of investigation may receive more emphasis than connections happened much earlier on due to the temporal locality of packet exchanges and network flows. We further use the topological structures as similarity measurement such as Jaccard coefficients and Katz measure, and integrate them into one coherent link anomaly methodology. Different types of anomalies are formally modeled by considering all combinations of previously unlinked/linked nodes and currently unlinked/linked nodes. In each time window, each pairwise nodes are assigned a normalized similarity score according to the aforementioned metrics and functions to measure their importance. The scores will be used to help determine whether the connections will be built or torn down in next time phase for a variety of situations. Based on the actual connectivity in a current snapshot graph, we are able to judge whether a link is anomalous or normal from the differences between the expected result and the reality.

On the other hand, the network data is usually highly dimensional with dozens of attributes. We further utilize these additional attributes in our anomaly analysis process. While one can use statistical or data mining processes to analyzes each of those dimensions of data, it is hard to correlate them in one coherent context for situation awareness. Choosing which attributes to examine can also be a daunting task and computationally infeasible for many automatic data analysis processes. Therefore, bringing domain experts into the loop through interactive visualization is promising. While there have been network management tools, few of them are lightweight enough and actually geared towards anomaly detection in dynamic traffic data. Motivated by this, we designed and implemented a generic network log analysis and visualization tool for situation awareness, anomaly detection and event investigation. The visualization tool incorporates four interrelated views, i.e., link anomaly graphs, parallel coordinates, treemaps, and Gantt charts. Each view is suitable for different characteristics of specific data attributes whether one would like to analyze the overall trend over time, distribution of values, or details-on-demand. The interactive features such as zoom-and-pan and linking-and-brushing allow investigators to connect dots together, analyze the network anomaly from different angles, and form a complete picture.

We evaluate our link anomaly detection algorithms by comparing our prediction with intrusion detection and prevention systems on publicly available datasets through metrics such as accuracies, true and false positives and negatives. Through extensive case studies using the visual analytic tool, we illustrate the effectiveness of the link anomaly algorithms and the network anomaly visualization framework.

Lingjia Liu – Dynamic Spectrum Access with Limited Sensing Capability; Electrical Engineering and Computer Science Department , University of Kansas

Dynamic spectrum access (a.k.a. cognitive radio) is regarded as one of the most promising technologies to efficiently increase the utilization of the available radio spectrum. Meanwhile orthogonal frequency division multiplexing (OFDM) becomes the dominant multi-access strategy for modern and future wireless systems due to the fact that it is flexible in allocating system resource and easy to implement. In a wireless system where the spectrum is accessed multiple users through OFDMA, a secondary user (SU) can flexibly utilize/share the “available” spectrum resource together with the primary user (PU) if the transmission of the secondary user can co-exist with the primary user. Accordingly, OFDMA based dynamic spectrum access received lots of attention from the research community.

Most of the existing work in cognitive radio networks is based on the assumption that secondary users can conduct spectrum sensing across all the carriers across all the subbands during a time-slot. In reality, there are a lot of constraints on the underlying processing capability of a cognitive radio secondary user, especially for small aircrafts such as UAVs. Accordingly, due to the hardware limitation, secondary users may have limited sensing capabilities, i.e., secondary users can only sense part of the spectrum and the sensing result may not always be perfect. In, a partially observable Markov decision process (POMDP) framework is introduced to solve the subband selection, sensing and spectrum access optimization problem in cognitive radio networks. The myopic subband selection policy that maximizes the immediate one-step reward is shown to be optimal in for the POMDP framework when the channel state of subbands transitions are positively correlated over time or the number of subbands is limited to two or three. Power allocation in cognitive radio network using the POMDP framework is considered in , however, the sensing result is assumed to be perfect. In [4], the problem of whether to sense and how long the SU should sense in an energy-constrained single-subband cognitive radio network is investigated using the POMDP framework.

In this report, we investigate communication strategies where SUs have limited sensing capabilities, i.e., SUs can only sense a portion of subcarriers within a subband. We will utilize spectrum sensing results developed from last year's Air Force Summer Faculty Fellowship Program (AF SFFP) together with machine learning techniques to characterize optimal sensing (subband and subcarrier selection, sensing time optimization, and optimal detections) and resource allocation for a cognitive radio network.

Jing Peng – View Based Regularization for Data Fusion (On Parzen Windows Classifiers); Computer Science Department, Montclair State University

Parzen Windows classifiers have been applied to a variety of density estimation as well as classification tasks with considerable success. Parzen Windows are known to converge in the asymptotic limit. However, there is a lack of theoretical analysis on their performance with finite samples. In this paper we show a connection between Parzen Windows and the regularized least squares algorithm, which has a well-established foundation in computational learning theory. This connection allows us to provide useful insight into Parzen Windows classifiers and their performance in finite sample settings. Finally, we show empirical results on the performance of Parzen Windows classifiers using a number of real data sets.

Gang Qu – A Survey on Memristor Modeling and Security Applications; Electrical and Computer Engineering Department, University of Maryland

With the recent advances in memristors as a potential building block for future hardware, it becomes an important and timely topic to study the role that memristors may play in hardware security. To address this issue, this paper presents a survey on research activities on memristor modelling and potential application of memristors in hardware security. First, we give an overview of the current literature on memristor experimentation, characterization, and modeling which includes Chua's original theoretical prediction model, more detailed models based on recent memristor implementations, and the SPICE simulation models. Then, we report the current research efforts on memristor-based security in three major areas: (1) memristor hardware primitives (e.g., physical unclonable function) that are based on the memristor effective resistance model, (2) encryption schemes that leverage the chaotic behavior of the memristor circuit, and (3) security concerns in memristor-based memory systems.

We observe that most of these works have limited scope and are based on simplified memristor models which diminish their practical value in security applications. Security applications have strict demands on repeatability, reliability, robustness, unforgeability, cost, resilience, and so on. To address these deficiencies, we propose a list of research areas that need to be addressed for building memristor-based security applications. We also analyze how memristors, as a new hardware building block, will impact major challenges in hardware security.

Walid Saad - Cyber-Defense Under Risk and Uncertainty: A Prospect-Theoretic Approach; Electrical and Computer Engineering, University of Miami

The primary goal of this extension grant was to develop a new mathematical framework, based on prospect theory, to study and analyze cybersecurity mechanisms in which there exists bounded rationality due to human decision making or to computational limitation. In particular, we have focused on studying, using prospect theory, cyber-defense mechanisms for hardware trojan detection.

The past decade has witnessed unprecedented advances in the fabrication and design of integrated circuits (ICs). Indeed, ICs have become an integral component in many engineering domains ranging from robotics to communication and power systems. These massive advances in IC design have also had many production implication. In particular, the flexibility of modern IC design coupled with its ease of manufacturing have led to the outsourcing of IC fabrication. Such outsourcing allows a cost-effective production of the IC circuitry of many of our nation’s most critical infrastructure. Moreover, the recent interest in the use of commercial off-the-shelf devices in both civilian and military infrastructure has also constituted yet another motivation for outsourcing IC fabrication.

Relying on offshore foundries for IC manufacturing is a cost-effective way for mass production of microcircuits. However, such an outsourcing can lead to serious security threats. These threats are exacerbated when the ICs in question are deployed into critical infrastructure such as a nation’s communication systems, power grid, or military settings. One such threat is that of the hardware trojan insertion by IC manufacturers. A hardware trojan is a malicious design that can be introduced into an IC at manufacturing. The trojan lies inactive until it is activated by certain pre-set conditions when the IC is in use. Once activated, the trojan can lead to a circuit error which, in turn, can lead to detrimental consequences to the infrastructure in which the IC is used. The threat of serious, malicious IC alterations via hardware trojans has become a major concern to government agencies, military, energy, and political sectors.

Defending against hardware trojans and detecting their presence faces many challenges that range from circuit testing and design to economic and contractual issues. The majority of these works focuses on IC and hardware-level testing procedures used to activate or detect hardware trojans.

This literature also highlights a key limitation in testing for hardware trojans: there exists a resource limitation that prevents testing for all possible types of hardware trojans within a given circuit. While interesting, most of these existing works do not take into account the possible interactions that can occur between the two entities involved in hardware trojan detection: the manufacturer of the IC and the recipient, such as the governmental agencies or companies that are buying the ICs. Indeed, there is a lack of a mathematical framework that allows to better understand the interesting interactions between these two entities. On the one hand, the manufacturer, viewed as an attacker, can strategically decide on which type of trojan to insert while taking into account possible testing strategies of the IC recipient. On the other hand, the agency, viewed as a defender, must decide on which testing process to use and for which trojans to test, given the possible trojan types that a manufacturer can introduce.

The main contribution of this extension grant was to propose a novel, game-theoretic framework to understand how the attacker and defender can interact in a hardware trojan detection game. The problem is formulated as a noncooperative zero-sum game in which the defender must select the trojan types for which it wishes to test while the attacker must select a certain trojan type to insert into the IC. In this game, the attacker aims to maximize the damage that it inflicts on the defender via the trojan-infected IC while the defender attempts to detect the trojan and, subsequently, impose a fine that would limit the incentive of the attacker to insert a trojan. One key feature of the proposed game is that it allows, based on the emerging framework of *prospect theory (PT)*, to capture the uncertainty and risk that accompany the hardware trojan detection decision making processes. This uncertainty and risk stem from the lack of information that the attacker and defender have on one another as well as from the possibly irrational behavior stemming from human involvement (e.g, system administrators at the defender and hackers at the manufacturer). Using PT allows to study how the attacker and defender can make their decisions based on subjective perceptions on each other's possible strategies and the accompanying gains and losses. Although game theory has been a popular tool for network security (see survey in, most existing works are focused on games in which all players are rational (one notable exception is in which, however, focuses on resource allocation and does not address hardware trojan detection). Moreover, beyond some recent works on using PT for wireless networking and smart grid, no work seems to have investigated how PT can impact system security, in general, and trojan detection, in particular. To solve the game under both standard, rational expected utility theory (EUT) and PT, we propose an algorithm based on fictitious play that is shown to converge to a mixed-strategy Nash equilibrium of the game. Then, for an illustrative numerical case study, we run several simulation results to better understand the implications of PT on security problems.

Shamik Sengupta – Insuring and Incentivizing Security Information Sharing: A Game Theoretic Perspective; Department of Computer Science and Engineering, University of Nevada, Reno

Rapid growth and strong backbone of internet technology has revolutionized the communication among individuals, firms, federal agencies and changed the way of conducting business by introducing e-business. Beginning from simple record keeping to military operations and highly secured business transactions are performed using networked systems. Therefore, widespread interconnectivity might give an opportunity to the malicious attackers in exploiting the firm's secured and private information to maximize financial gain. These kind of security breaches in loosely secured systems are very harmful to both firms & their customers and poses unprecedented national risk too. Some recent cyber attack victims, U.S. based famous retail shops, Target Corp, Neiman Marcus have been breached on the holiday season and reported that approximately 70 million payment card numbers & at least 70 million customer information have been stolen. Washington state administrative office of the courts was compromised in the early 2013 that exposed 160K social security numbers and 1 million driving licenses. JP Morgan Chase & Co was reportedly breached by cyber criminals and found that 2% of its UCard user's personal information was temporarily appeared in plain text instead of encrypted/scrambled format in their log files. The famous media company NBC.com was a victim of cyber attack by a sophisticated Citadel malware which was designed for bank fraud and cyber espionage. From past decade the cybercrime has raised to its topmost level and the severity of security breaches can lead to complete breakdown of supported infrastructure along with firm's business.

Isolated research on cyber security threats analysis and developing anti-threat strategies by individual firms may not be a cost-effective way to tackle cybercrimes. For instance, when a firm finds it has been compromised by an attacker, it tries to develop a countermeasure at the earliest by investing money and time. At the same time some other organization that had faced the same attack in past would have already developed countermeasure for the breach. From many past cyber attacks, it has been figured out that exchange of security information related to attacks, unsuccessful attempts, expected breaches etc., can be an effective way for firms to collaboratively beef up their security infrastructure. However, firms hesitate to share their security information with other federal agencies and firms as the outside world and the customers might perceive the attack in a negative sense which might tarnish firms' reputation resulting in loss of market share and overall revenue, thus deterring the firms from disclosing such information or share collaboratively. However, vulnerability information sharing has more benefits for the firms such as: (1) prevention of future cyber attacks, and revenue loss by finding and repairing the vulnerabilities, (2) sharing breach information to a standardized central monitoring system governed by federal agencies can be a strong reason to assure its customers about its action on security measure which will allay the customers' perceived security risk, (3) cost of investment in developing countermeasure to cyber attack is more compared to collaborative effort on hardening security technology. Cyber security information exchange can be difficult unless there exists proper information exchange framework and globally common message format. Therefore, President's executive order attempted to address such threats and develop protective countermeasures by defining legislative & constitutional authority for the executive order which will set the right tone and balance between cyber protection, breach sharing, and individual privacy. To enable the security information sharing, ITU-T took initiative to adopt a cyber security information exchange (CYBEX) that imports more than twenty best standards developed by different agencies to harden the cyber security and infrastructure protection. CYBEX framework aims to provide service of structured information exchange about measurable security states of systems/devices and incidents on cyber attacks along with its severity level.

Several critical issues must be addressed for the breach-sharing firms to motivate them towards reporting and disseminating the breach related information. In this research, we aim to devise an economic incentive mechanism based on game theory for the competing firms on sharing vulnerability information to each other and also to the central information exchange. Economic theories have recently been used extensively to analyze numerous networking and communications problems where interacting decision-makers have conflicting objectives. Recently, game theories have been shown to be powerful tools to deal with cyber attack problem and information sharing in PI’s prior research and other works This is because the service quality (utility) that each user receives in a competitive environment is often affected by the action of other users who also try to contend for the same pool of resources thus making gametheoretic tool to be an ideal candidate to analyze the conflicting scenarios. Lack of such a model is not only because security information exchange frameworks are still in their infancy, but also because of the complexity arising from the inter-dependent multi-layer competitions and various incentive factors. In this research, we raise questions and seek answers on how to design decision mechanisms that can lead the firms decide the optimal level of information sharing & security investment to maximize their robustness and in turn minimize their cyber-insurance premium.

Pramod K. Varshney – A Framework to Implement the Cyber Survive and Recover Simulator (CSRS) Demo Electrical Engineering and Computer Science Department, Syracuse University

Systems in the real world are always prone to attacks, resulting in components or sub-systems to fail, thereby preventing the overall goal of the system to be met. A solution technique is to design attack-tolerant cyber systems that can survive and recover by having multiple redundant components which can be used when some components fail. Further, by having components of different types (i.e., diverse components immunity of the system to attacks can be further increased. Diversity, though potentially helpful for designing more robust and survivable systems, comes at a price- it reduces inter-operability of systems, and increases overall maintenance costs. Having similar individual components in a system ensures seamless interconnectivity. Further, maintenance costs (training costs of personnel etc.) of such homogenous systems are also less. Thus, while designing a system, it is critical to strike the correct balance between having a monoculture, i.e., a homogenous system (to maximize interoperability) and having a diverse system comprised of varied components (to reduce security loss). The strategic decision variable is the level of diversity, with interoperability and security risk as the main tradeoff.

The objective of the proposed effort is to develop a software tool that will facilitate analysis of strategic use of redundancy and diversity techniques for cyber survivability and recoverability against tactical attacks by leveraging Game Theoretic concepts. The demo shows the potential of using game theoretic approaches for exploiting diversity for cyber survivability. The basic demo so far considers a simple two player (an attacker and a defender) cyber survivability game solvable as a one shot normal form complete information game.

Jian Tang – Survivable Online Stream Data Processing in a Cloud; Center for Science and Engineering (CASE), Syracuse University

In this project, we focus on a large-scale data processing system running in a cloud with multiple geo-distributed Data Centers (DCs). Managing virtual resources and supporting survivability across multiple geo-distributed DCs are very challenging since Virtual Machine (VM) synchronization and live migration over a WAN are very difficult and costly due to long communication delay, addressing and reliability issues. We employ a different approach here which determines how to provision virtual servers, distributes requests and data for each application to meet the requested Service Level Agreement (SLA) before failures, and re-distributes service requests and data among surviving DCs to satisfy the same (without performance degradation) or slightly relaxed (with graceful degradation) SLA constraints after failures. We consider a regional failure model in which one or multiple DCs may fail simultaneously.

Specifically, we study a Virtual Server Provisioning and Selection (VSPS) problem in distributed DCs with the objective of minimizing the total operational cost while meeting the service response time requirement. We aim to develop general algorithms for the VSPS problem without assuming a particular queueing model for service processing in each DC. First, we present a Mixed Integer Linear Programming (MILP) formulation. Then we present a 3-step optimization framework, under which we develop two polynomial-time ln(*N*)-approximation algorithms (where *N* is the number of clients) as well as a fast heuristic algorithm. We also show this problem is NP hard to approximate and is not possible to obtain a better approximation ratio unless NP has TIME ($n^{O(\log \log n)}$) deterministic time algorithms. In addition, we present an effective algorithm that jointly obtains the VS provisioning and selection solutions. Extensive simulation results are presented to justify effectiveness of the proposed algorithms.

University of Central Florida (Mainak Chatterjee) – Demo: Exploiting Diversity for Survivability of Cyberspace; Department of Electrical Engineering and Computer Science, University of Central Florida

In this project, we characterize the QoS that secondary users can expect in a cognitive radio network in the presence of primaries. To that end, we first define a *K*-dimensional QoS space where each point in that space characterizes the expected QoS. We show how the operating condition of the system maps to a point in the QoS space, the quality of which is given by the corresponding QoS index. To deal with the real-valued QoS space, we use vector quantization to partition the space into finite number of regions each of which is represented by one QoS index. We argue that any operating condition of the system can be mapped to one of the pre-computed

QoS indices using a simple look-up in $O(\log N)$ time– thus avoiding any cumbersome computation for QoS evaluation. The proposed technique takes the power vector as its input from the power control unit which we consider as a black box. Using simulations, we illustrate how a K-dimensional QoS space can be constructed. We choose capacity as the QoS metrics and show what the expected capacity would be for a given power vector. We also show the effect of having large number of partitions on the distortion. As for the implementation feasibility of the proposed concept, we implement the QoS space on an 8-bit microcontroller and show how the mathematically intensive operations can be computed in a short time. Further we use binary search to achieve scalability as the dimensionality of the space increases.

Venkat Venkateswaran – Modeling Health Infrastructure in the NOEM Health Module; Department of Engineering and Science, Rensselaer Polytechnic Institute at Hartford

The National Operational Environment Model (NOEM) is a large scale stochastic model that can be used to simulate the operational environment of a nation-state. The model will recreate in software the main attributes of the nation under study. Intelligence analysts and decision makers will then be able to examine the effects of various action alternatives through simulations. NOEM has several interworking components devoted to modeling different aspects of a nation like its demographics, economy and so forth. The Health Module is one such module and attempts to capture the health dimension. While hospitals are never targeted they may however be adversely affected when lifeline services like water supply and power are disrupted. In NOEM hospitals are modeled as demand centers that draw inputs (water, power, communication services) from NOEM infrastructure elements. In a simulated attack on these elements hospitals will be bereft of these lifeline inputs and left incapacitated. We want to model the resulting impacts of such events. In this report we develop a model based on empirical findings from published research to compute the DALY burden resulting from lifeline outages. DALY, or disease adjusted life years lost, is a metric to capture not only mortality but the disability burden from less-than-normal productive life. In addition researchers have found that power outages cause measurable excess deaths across disease groups. We have incorporated this effect also in our model. We also wanted to investigate if at the national level for countries there is a correlation between the number and quality of health care infrastructure and manifest health performance indicators like mortality rates. To that end, we analyzed data from several LMIC (low and middle income countries) from the AFR, AMR, EMR and SEA WHO-regions. We find that there is significant correlation between the response variables of overall death rate, death rates for TB, communicable diseases mortality proportion and maternal mortality and the predictor variable of per capita number of physicians in the country (adjusted R^2 ranging from 54% to 74%). Of several potential health infrastructure predictors tested the per capita number of physicians appears to be the only predictive variable in this regard.

Michael Wicks – MIMO Communications for Signal Separation and Space-Time Encryption, Department of Electrical and Computer Engineering, University of Dayton

Space-time encryption and encoding employing edge-of-the-art connectivity and dissemination technology offers an extension of traditional encoding and one-dimensional public key encryption techniques to yield coded data that is four dimensional (represented by a matrix composed of time plus the three dimensions of space) instead of one dimensional data (a time domain or frequency domain data vector). Classically, encryption is a process for the transformation of a stream of data (a data vector or vectorized data set) into cipher text (another vector) which is not discernable by individuals without the prior knowledge contained in a decryption key. Decryption is the process by which cipher text is converted into a form which is a reasonable facsimile of the original data. A key is required to recover the original data through decryption. Sophisticated algorithms resulting in strong encryption are essential in this era in which high performance computers are used to decode cypher text without the appropriate key. Strong encryption is especially important in an era of wireless communications for connectivity and dissemination.

Xuanhui Wu – MIMO Antennas for a Terrestrial Point-to-Point Wireless Link: From the Optimum Antenna Spacing to a Compact Array; Department of Electrical and Computer Engineering and Technology, Minnesota State University

Multiple-input-multiple-output (MIMO) antenna technology has been proven to tremendously increase wireless communication systems' capacity without extra frequency bandwidth. It relies on rich scatters in the wave propagation environment to construct virtually independent sub-channels. For a MIMO link, the received signals are

$$s_r = Hs_t + n$$

where s_t is the transmit signal vector, s_r is the received signal vector, H is the channel matrix, and n is the noise vector. In a rich scattering environment such as urban areas, the channel matrix is well conditioned and the transmitted data can be recovered as

$$s'_t = H^{-1}s_r$$

The idea of using multiple antennas to increase data is also introduced to terrestrial microwave links. However, for a terrestrial point-to-point wireless link as shown in Fig. 1, the channel is dominated by line-of-sight paths and possibly additional ground reflection paths. The lack of scatters in such a channel may result in a ill conditioned channel matrix, and the computation of (2) becomes unreliable. Repeaters can be used to improve the condition of the channel matrix, but it requires expensive upgrade of the infrastructure. At millimeter wave frequency, MIMO technology is implemented for a line-of-sight short distance communication.

Without scatters, a proper arrangement of antennas' positions may produce a well behaved channel matrix. A 2×2 terrestrial MIMO link is shown in Fig. 1, with tower height T=50m, tower to tower distance D=50km, carrier frequency of 850MHz, 30dB signal to noise ratio (SNR) and a quadrature phase shift key (QPSK) modulation scheme. Fig. 2 shows the received constellation diagram for different antenna spacing if (2) is applied. Clearly, in order to achieve a low bit error rate (BER), a spacing of 30m is required for this example, which is impractical.

This paper investigates the performance of a terrestrial point-to-point MIMO link. Our study is carried out by exploring the channel condition number, channel capacity and the BER performance of a communication link. The channel model incorporates wave propagation phenomena such as ground reflection and polarization mismatch. In Section 2, the effects of

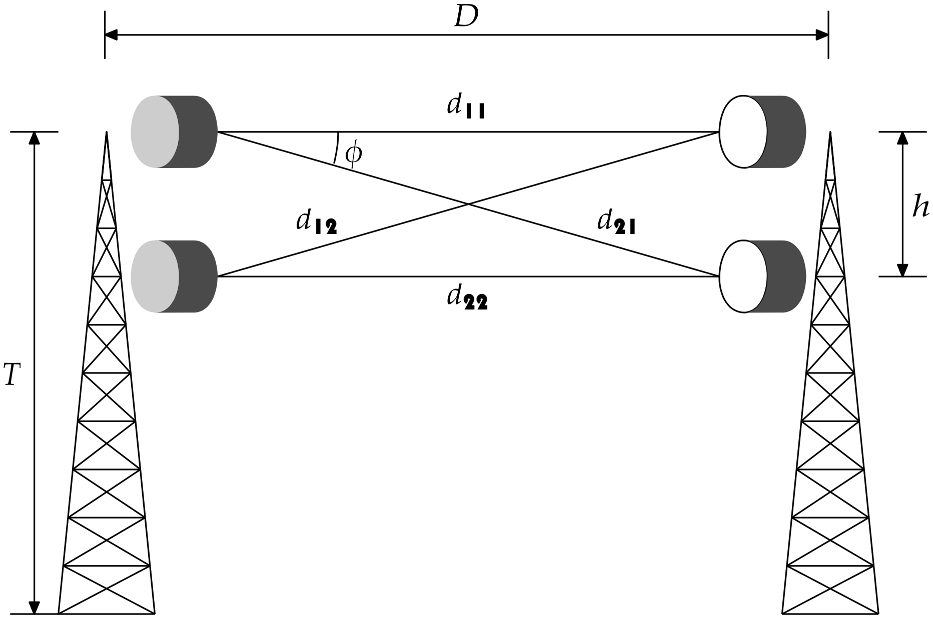

Figure 1: A 2 × 2 terrestrial MIMO link.

antenna spacing on the condition number of the channel matrix and BER performance are studied. Both long range and short range links are discussed. Section 3 presents an 8 × 8 MIMO link. It is implemented by deploying four dual-polarized antennas at both the transmitting and receiving sides. The condition when the ground reflection should be considered is discussed. The channel matrix is derived using a two-path model, and polarization mismatch is incorporated in the model. The condition number of the channel matrix and the capacity of the channel is examined. Section 4 presents a constellation multiplexing technique to avoid the unreliable result of (2) when compact antenna arrays are deployed. Excellent BER performance is observed.

Yang Yi – Neuron Design in Neuromorphic Computing Systems and its Application in Wireless Communications; Computer Science and Electrical Engineering, University of Missouri - Kansas City

As semiconductor technologies continue to scale further into the nanometer regime, it is important to study how non-traditional computer architectures may be uniquely suited to take advantage of the novel behavior observed for many emerging technologies. Neuromorphic computing systems represent a type of non-traditional architecture encompassing evolutionary. Neuromorphic computing systems hold great promise for many important engineering and scientific applications. Such systems exhibit rich dynamical behaviors within a simple architecture, and are capable of high speed parallel signal processing. In recent years, the research on neuromorphic computing has made swift progress and development in theoretical study and hardware implementations, but one of the major challenges to its implementation lies in the development of suitable data representation for sensory information in neuronal activities.

This project is to develop novel and fundamental methodologies for data representation using hardware spike timing dependent encoding and explore the applications of neuromorphic computing in wireless communications. In this extension, we expanded our previous work that patterns the neural activities on multiple timescales and encodes the sensory information using temporal scales. The spiking encoding methodologies for autonomous classification of time series signatures will be further explored using near chaotic reservoir computing. Furthermore, we explored the application of reservoir computing in wireless communications including Multiple-Input and Multiple-Output (MIMO) channel equalization and channel estimation. The extension project focus on the architectural design and testing of spikey time encoding circuits that explore how artificial computational systems can utilize the sensory encoding methodologies employed in biological brains.

Heng Yin – Automated Document Parser Generation Through Binary Code Reuse; Electrical Engineering and Computer Science, Syracuse University

In an environment like Air Force, users exchanges documents in their daily operations. These documents need to be properly examined and sanitized, especially when the documents are exchanged between two security levels. A high-fidelity parser is needed to correctly examine the document structure and enumerate the document objects. However, developing a good parser is hard, because document specifications are complex and often vague, leaving a big semantic gap between a over-simplified parser in security scanners and highly complex parser in real document processors. Attackers can exploit this semantic gap to launch chameleon attacks and werewolf attacks.

To close this semantic gap, we propose a new a technique for automated parser generation. The basic idea is to reuse the parser functionality in a real document processor. More specifically, we constructed a PDF parser program by directly reusing the document parsing functionality in Adobe reader. We first developed a new dynamic binary analysis technique to automatically identify the hook point in Adobe Reader for retrieving JavaScript code from a PDF document. We then directly patch the Adobe Reader and turn the patched program into a PDF parser. We evaluated this parser with over 11,000 malicious PDF files and compared with a widely used PDF parser tool called **pdfextract**. Our experiment demonstrated the advantage of our PDF parser: it extracted JavaScript code in over 300 PDF documents, which **pdfextract** failed to extract.

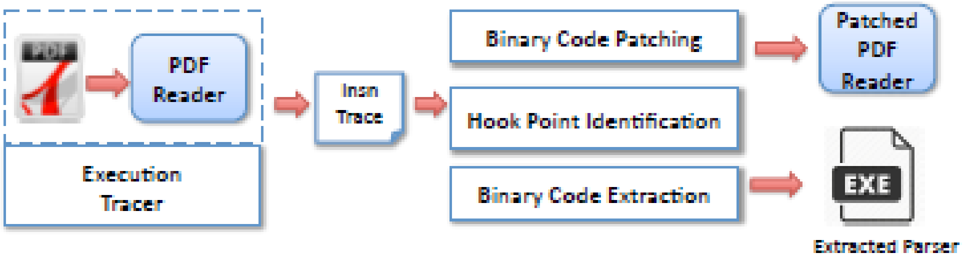

Figure 1: Parser generation through binary code reuse

<u>Ming Zhao – Elasticity and Eeconomics of Cloud Computing; School of Computing and Information Sciences, Florida International University</u>

The elasticity and economics of cloud computing offer significant benefits to mission-critical applications which are increasingly complex and resource demanding. Clouds also provide powerful tools such as virtual machine (VM) based replication and migration for defending mission-critical applications. However, cloud-based mission-critical computing raises serious challenges to mission assurance. VM-based consolidation brings different applications to the same set of physical resources, increasing the risk of one user compromising the mission of another. For example, although it is straightforward to protect the contents of VM communications by encrypting the messages, the communication patterns among mission-critical VMs can still be discovered by malicious VMs on the same cloud network and exploited to identify and attack the high-value targets. Nonetheless, the mission-critical application in a VM lacks the visibility and control to detect and stop such attacks, whereas the support for security isolation from existing cloud systems is also limited.

The objective of this 2014 summer extension project is to address these challenges and improve the mission assurance of applications in clouds through the novel use of virtual networks for protecting the communications among mission-critical VMs. Specifically, this project studied a new attack avoidance approach by masquerading the communications among mission-critical VMs on a shared cloud network, thereby improving the mission assurance of applications from attacks in clouds. Center to this approach is a new virtual-network-based message forwarding technique which forms a peer-to-peer (P2P) based virtual network among the mission-critical VMs and masquerade the VM communication patterns by forwarding the messages through the peer VMs on the virtual network. This technique is implemented on OpenStack, a widely used cloud computing platform, and IP over P2P (IPOP), a flexible virtual networking framework. It can be combined with the VM-migration-based moving-target defense technique studied by the PI in summer 2014 to provide avoidance of a variety of co-residency and network attacks in cloud systems.

2.3. 2015 Extension Grants

Vaneet Aggarwal – Data Completion: Fundamental Limits and Algorithms; School of Industrial Engineering, Purdue University

In this work, we first consider the case where the columns of the matrix can be grouped (clustered) into subspaces (not necessarily disjoint or independent), and give novel algorithms for data completion. Further, we consider the use of alternating minimization rather than convex relaxation for multi-dimensional data completion. The report is divided in two sections. The first gives proposes and analyses a feasible algorithm for union of subspaces model, and the second considers multi-dimensional data completion using alternating optimization.

Howard A. Blair, – Verification and Validation of Coupled Quantum/Classical Programs; Department of Electrical Engineering and Computer Science, Syracuse University

During the VFRP summer period, we developed analysis, specifically differential calculus, on continuous domains, in agreement both with differential calculus on the continuous domain of real closed and bounded intervals, situated in relation to mainstream domain theory, and in agreement with differential calculus on convergence spaces, therefore in agreement with elementary differential calculus on Euclidean and Hilbert spaces, the latter being essential for the formal semantics of quantum programming languages. Differential calculus on such structures allows a specification logic with a rigorous mathematical semantics for formal approaches to verification of heterotic quantum/classical programs. Our previous work based on ordinary differential equations over convergence spaces needed to be extended to treat specific programming language constructs, not merely their representation as formal heterotic dynamical systems, and therefore needed to be aligned with developments in mainstream domain theory that underlays specification logics in formal methods of verification and validation. Previously developed work on differential calculus on convergence spaces was specifically applied to constructing a differential calculus on the real interval domain and to differentiation of interval-valued functions of a real variable so as to provide a rigorous basis for continuous-time dependent dynamical systems with real interval-valued variables. To specifically obtain a semantically rigorous verification logic based on domains, we needed to be able to capture the continuous-time unitary evolution of quantum states seamlessly combined with discrete-time evolution of classical states. Pursuant to this goal we further developed the notion of *differential* on the Scott domain of real-number intervals Edalat and Lieutier, Blair, et al.,Martin and Panangaden, Patten, and Patten, et al., developed the notion of differential for interval-valued functions of a real variable thus enabling us to have continuous-time evolution of interval-valued functions characterized by time-dependent ordinary differential equations involving interval-valued variables, a variation of Boolean differentiation based on the Galois field GF with respect to which a discrete analogue of the notion of Hermitian operator is obtained, from which we obtain in turn a discrete notion of the time-dependent Schrödinger equation.

In the next section, will provide technical background on

1. convergence spaces
2. why domains?
3. Scott domains, the set of real numbers as a Scott domain
4. the interval domain generated by the real numbers, IR and half-plane representation
5. Boolean differentiation using GF.

This technical background is also presented in.

Soundararajan Ezekiel – Multi-Resolution Fusion & Advanced Fusion Performance Evaluation Tool for AI based Natural Language Annotation Engine for Video Imagery Sources; Computer Science Department, Indiana University of Pennsylvania

To develop a novel multiresolution fusion and advanced fusion performance evaluation tool for an Artificial Intelligence based natural language annotation engine for video imagery sources using three-dimensional Receiver Operating Characteristic (ROC) curve and Area Under the Curve (AUC), proposed for extension grant work. The proposed system consists of four goals:

1. Continue to work on AI based natural Language Annotation Engine for Video Imagery source
2. Contourlet/Bandelet Transformation Based Image Registration
3. Continue to work on Multi-resolution fusion using *-let transformations
4. ROC Curve Analysis for Validating Objective Image Fusion Metrics

Daqing Hou – Web Browser Extension Development and Data Extraction; Electrical and Computer Engineering Department, Clarkson University

This extension grant research project is focused on the initial design and prototyping of the idea of “data transposition,” a term coined by AFRL’s Mr. Michael Manno, as part of the Firefox addon called Atlas Extension (AE). Briefly, data transposition refers to the software capability of recording the multiple manual steps involved in searching for an information item of interest using the browser, converting them into a named process, and lastly, automatically applying this created process to similar information seeking tasks in future. For example, we would like to be able to transposition from a task of finding tuition, location, and population for Clarkson University to finding the same information for St. Lawrence University or RPI. Another example would be the transpositioning of a trip planning process for the tourism destination Disneyland Hotel in CA to one for Great Wolf Lodge PA. If a transpositioned process uses the same data sources as in the recorded initial manual search, we call it a direct transposition. The college search process above would be such an example. Otherwise, it is called an indirect data transposition.

Our focus for this extension grant is on direct data transposition, due to its relative simplicity. Our main conclusion is that direct data transposition is technically feasible. The following functionalities for supporting direct data transposition have been prototyped for AE as an outcome of this effort: the ability for AE to automatically record a new URL visited by the user, a new notational design for modeling the input/output relationship between the multiple steps of a process, and a new user interface that for the first time demonstrates a truly automated direct data transposition. A user/design manual is provided to support future users and developers.

Jai (Kevin) Liu – Understanding Delay Performance of Massive-MIMO Downlink Scheduling with Finite CSI Feedback Rates; Department of Electrical and Computer Engineering, The Ohio State University

In this research, we study the impact of finite-rate CSI feedback on queueing delay in Massive MIMO cellular downlink. The contribution of this research is that we conduct an in-depth theoretical study on the impact of finite-rate CSI feedback in M-MIMO networks on the queueing delay performance of the widely adopted queue-length-based back-pressure joint congestion control and scheduling algorithm. We first establish an analytical framework that captures the essential interactions between physical layer radio resource and the scheduling/congestion control decisions in M-MIMO-based cellular networks. This analytical framework facilitates tractable and accurate modeling that enables our subsequent analytical analysis on queueing delay in M-MIMO cellular networks. Based on the proposed analytical framework, we study how the delay performance of the widely adopted queue-length-based back-pressure joint congestion control and scheduling algorithm is affected by *any B*-bit finite-rate CSI feedback used in Massive MIMO cellular networks. Interestingly, we theoretically establish a sufficient condition on the scaling of \$B\$ such that the queueing delay scaling *remains the same* compared to the perfect CSI cases. Our results contribute to an exciting new research area in M-MIMO design and optimization theory for future 5G wireless communications.

Rong Pan – Detecting Communities by Sentiment Analysis of Controversial Topics; School of Computing, Informatics, and Decision Systems Engineering, Arizona State University

Controversial topics, particularly political topics, often provoke very different emotions among different communities. By detecting and analyzing communities formed around these controversial topics we can paint a picture of how polarized a country is and how these communities evolved over time. In this research, we made use of Internet data from Twitter, one of the most popular online social media sites, to identify a controversial topic of interest and the emotions expressed towards the topic. Communities were formed based on Twitter user's sentiments towards the topic. In addition, the network structure of these communities was utilized to reveal those Twitter users that played important roles in their respective communities.

Venkat Venkateswaran – Modeling Failures in Power Grids; Department of Engineering and Science, Rensselaer Polytechnic Institute

This work addresses modeling of failures in power grids. The Restoration Problem is the problem of rerouting power flows and adjusting generator capacities optimally to restore as much of the supply as possible in the event that certain network elements (nodes and/or links) are damaged. In this work we have enhanced our earlier algorithm using sparse constraint techniques so that it can solve problems with about 4000 nodes and 7000 links. This is thought to be the size of networks (such as the Texas Network) that may be required to be analyzed by the National Operational Environment Model (NOEM). We report on test results with numerous random problems of the above dimensions. We mention that in each and every case the algorithm successfully found the optimal solution thereby confirming that the it can handle large problems of this size. The computation times appear reasonable and the algorithm appears quite robust. Our algorithm makes use of commercial optimization software IBM CPLEX. We also investigated the viability of using open source optimization software instead. GLPK distributed under the GNU project appears to be the most attractive option. However we do not have any test results to report for we have not yet been able to successfully debug and use the code at this time.

Meng Wang – Event Identification for Network Monitoring Based on Subspace Analysis; Department of Electrical, Computer, and Systems Engineering; Rensselaer Polytechnic Institute

The monitoring of Air Force information systems and networks requires the ability to accurately extract information from large volumes of measurements. Through the Visiting Faculty Research Program, we studied the missing data recovery problem for network monitoring when the complex network experiences multiple events. Building on our obtained results, we further explore the event identification problem. We develop computational efficient methods to detect, locate, and identify the events. The central idea is to exploit the low-dimensional structures in the high-dimensional measurements that result from the underlying dynamic system.

3. EXPENDITURES

Under this contract expenses were billed on a faculty/week basis. The rates for the professors were established by the National Research Council for summer research fellows and are as follows.

3.1. Faculty Labor

<u>2013 – 2014</u>

Assistant Professor	$1,300/week
Associate Professor	$1,500/week
Full Professor	$1,700/week
Faculty Per Diem:	$50/day up to $250/week

<u>2015</u>

Assistant Professor	$1,500/week
Associate Professor	$1,700/week
Full Professor	$1,900/week
Faculty Per Diem:	$70/day up to $350/week

*Faculty members whose home residence/university is more than 50 miles from AFRL/RI were entitled to Per Diem

3.2. Other Costs Associated with Program

<u>2013-2014</u>

Round trip travel reimbursement at the start and completion of the project not to exceed $1000 was provided as requested.

<u>2015</u>

Round trip travel reimbursement at the start and completion of the project not to exceed $1500 was provided as requested.

4. LIST OF ACRONYMS

ABW – Air Base Wing

AE – Atlas Extension

AFB – Air Force Base

AFR – African

AFRL – Air Force Research Laboratory

AI – Artificial Intelligence

AIPR – Applied Imagery Pattern Recognition

AMR – Americas

ANN – Artificial Neural Network

A-NoC – Analog Network-on-Chip

AUC – Area Under the Curve

AV – Audio/Video

AVI – Approximate Value Iteration

BER – Bit Error Rate

BIO-AI – Biological Artificial Intelligence

BSB – Brain-State-in-a-Box

C2 – Command and Control

CA – California

CASE – Center for Science and Engineering

CBIR – Content-Based Image Retrieval

CDL – Common Data Link

CEP – Complex Event Processing

CNA – Critical Node Analysis

CODED – Component-Oriented Data Encryption and Deduplication

CPLEX – C Programming Language Simplex Method

CPS – Cyber-Physical Systems

CPU – Central Processing Unit

CR – Cognitive Radio

CSI – Channel State Information

CSRS – Cyber Survive and Recover Simulator

CSS3 – Cascading Style Sheets Level 3

CYBEX – Cyber Security Information Exchange

DALY – Disability-Adjusted Life Year

DBMS – Database Management Systems

DC – Direct Current

DC – District of Columbia

DoS – Denial of Service

DSA – Dynamic Spectrum Access

DTIC – Defense Technical Information Center

EMR – Eastern Mediterranean Region

ESN – Echo State Neural Networks

EUT – Expected Utility Theory

FIRE – Fast, Inexpensive, Reliable, and Easy-to-use

FMV – Motion Video

FQI – Fitted Q-Iteration

GCS – Ground Control Station

GDELT – Global Database of Events, Language, and Tone

GF – GeForce

GLPK – GNU Linear Programming Kit

GNU – GNU’s Not Unix

GPS – Global Positioning System

HIFC – High-Speed Integrate-And-Fire Circuit

HIS – Hyperspectral Imaging

H-O-M – Hong-Ou-Mandel

HTML5 – HyperText Markup Language Hyper Level 5

HTTP – Hypertext Transfer Protocol

IBM – International Business Machines

ID – Identification

IEEE – Institute of Electrical and Electronics Engineers

IF – Image Fusion

IFC – Integrate-and-Fire

IP – Internet Protocol

IPOP – Internet Point of Presence

IR – Infrared

ITU-T – International Telecommunication Union - Telecommunication Standardization Sector

JPEG – Joint Photographic Experts Group

LMIC – Low and Middle Income Countries

LOQC/QIP – Linear Optical Quantum Computing and Quantum Information Processing

MAC – Macintosh

MBC – Memristor-Based Crossbar

MBSA – Multiple Beam Smart Antennas

MCC – Mobile Cloud Computing

MDP – Markov Decision Process

MI – Mutual Information

MILP – Mixed Integer Linear Programming

MIMO – Multiple-Input Multiple-Output

MIP – Mixed Integer Programs

MMB – Markov Model Bank

MS – Microsoft

MTD – Moving Target Defense

MTDG – Moving Target Defense With Guarantees

NBC – National Broadcast Company

NCA – Neuromorphic Computing Accelerators

NFC – Near Field Communication

NOEM – National Operational Environment Model

NP – Network Protocol

OFDM – Orthogonal Frequency Division Multiplexing

OS – Operating System

PA – Pennsylvania

PC – Personal Computer

PDF – Portable Document Format

PHY-AUR – PHYsical layer Authentication with Untrusted Relay

PHY-CRAM – Physical Layer Challenge-Response Authentication Mechanism

PHY-CRAMR – Physical Layer Challenge-Response Authentication Mechanism Relay

PHY-MPA – Physical Layer Multipath Challenge-Response Authentication

PI – Principle Investigator

POMDP – Partially Observable Markov Decision Process

PT – Prospect Theory

PU – Primary User

QLA – Queue-Length-Based Algorithms

QoS – Quality of Service

QPSK – Quadrature Phase Shift Key

Q-RAM – Quantitative Risk Analysis and Measurement

RLC – Rate Loss Constraint

ROC – Receiver Operating Characteristic

RPI – Rensselaer Polytechnic Institute

SAW – Situation Awareness

SBVLC – Secure Barcode-based Visible Light Communication

SEA – South-East Asia

SEP – Stream and Event Processing

SLA – Service Level Agreement

SMS – Short Message Service

SNR – Signal to Noise Ratio

SOA – Service Oriented Architecture

SOAP/HTTP – Simple Object Access Protocol/Hypertext Transfer Protocol

SP – Stream Processing

SPICE – Simulation Program with Integrated Circuit Emphasis

SSID – Service Set Identification

SSIM – Structural Similarity Index

SU – Secondary User

SUNY – State University of New York Polytechnic Institute

SWaP – Size, Weight, and Power

TB – Tuberculosis

UAV – Unmanned Aerial Vehicle

UI – User Interface

URL – Uniform Resource Locator

US – United States

VFRP – Visiting Faculty Research Program

VM – Virtual Machine

VMR – Visual Media Reasoning

VMR/CBIR – Visual Media Reasoning Content-Based Information Retrieval

VNR – Visual Media Reasoning

VRUS – Vulnerable Road User Safety

VS – Virtual Server

VSPS – Virtual Server Provisioning and Selection

WAM – Wide Area Motion Imagery

WAN – Wide Area Network

WHO – World Health Organization

WS – Web Services

WS-* – Web Services-Star

XSS – Cross-Site Scripting